FEDERAL COMPUTER SECURITY MARKET

1992 - 1997

INPUT

About INPUT

INPUT provides planning information, analysis, and recommendations for the information technology industries. Through market research, technology forecasting, and competitive analysis, INPUT supports client management in making informed decisions.

Subscription services, proprietary research/consulting, merger/acquisition assistance, and multiclient studies are provided to users and vendors of information systems and services. INPUT specializes in the software and services industry which includes software products, systems operations, processing services, network services, systems integration, professional services, turnkey systems, and customer services. Particular areas of expertise include CASE analysis, information systems planning, and outsourcing.

Many of INPUT's professional staff members have more than 20 years' experience in their areas of specialization. Most have held senior management positions in operations, marketing, or planning. This expertise enables INPUT to supply practical solutions to complex business problems.

Formed as a privately held corporation in 1974, INPUT has become a leading international research and consulting firm. Clients include more than 100 of the world's largest and most technically advanced companies.

INPUT OFFICES

North America

San Francisco
1280 Villa Street
Mountain View, CA 94041-1194
Tel. (415) 961-3300 Fax (415) 961-3966

New York
Atrium at Glenpointe
400 Frank W. Burr Blvd.
Teaneck, NJ 07666
Tel. (201) 801-0050 Fax (201) 801-0441

Washington, D.C.
INPUT, INC.
1953 Gallows Road, Suite 560
Vienna, VA 22182
Tel. (703) 847-6870 Fax (703) 847-6872

International

London
INPUT LTD.
Piccadilly House
33/37 Regent Street
London SW1Y 4NF, England
Tel. (071) 493-9335 Fax (071) 629-0179

Paris
INPUT SARL
24, avenue du Recteur Poincaré
75016 Paris, France
Tel. (33-1) 46 47 65 65 Fax (33-1) 46 47 69 50

Frankfurt
INPUT LTD.
Sudetenstrasse 9
D-6306 Langgöns-Niederkleen, Germany
Tel. (0) 6447-7229 Fax (0) 6447-7327

Tokyo
INPUT KK
Saida Building, 4-6
Kanda Sakuma-cho, Chiyoda-ku
Tokyo 101, Japan
Tel. (03) 3864-0531 Fax (03) 3864-4114

M&S 459/01 5/91

APRIL 1992

FEDERAL COMPUTER SECURITY MARKET

1992-1997

INPUT®

1953 Gallows Road, Suite 560, Vienna, Virginia 22182 (703) 847-6870

Published by
INPUT
1953 Gallows Road, Suite 560
Vienna, VA 22182-3934
U.S.A.

Federal Information Technology Market Program (FITMP)

Federal Computer Security Market, 1992-1997

FISE2 • 499 • 1992

Abstract

INPUT expects the federal government market demand for computer security products and services (excluding network security) to grow from $609 million in FY 1992 to $761 million in FY 1997. This represents a compound annual growth rate (CAGR) of 5%. This estimate excludes classified processing, since that data cannot be captured.

Federal Computer Security Market, 1992-1997 covers the forces, both positive and negative, driving this market. This report revisits research pertaining to this market conducted in 1990 and cites few significant changes. It also identifies which agencies will buy, how much will be bought, how it will be bought, and who will do the buying. The report compares agency and vendor perceptions of the market, and suggests some steps for vendors to take in expanding their market share.

This report contains 160 pages including 66 exhibits.

Table of Contents

Table of Contents (Continued)

Table of Contents (Continued)

Table of Contents (Continued)

Appendixes

Exhibits

Exhibits (Continued)

IV

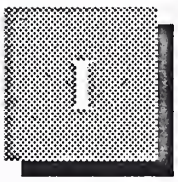
V

Exhibits (Continued)

V

Appendixes

B



Introduction

The *Federal Computer Security Market, 1992-1997* is an update of INPUT's 1990 report concerning the market for security of federal information systems containing sensitive (but typically unclassified) information. The report was prepared in response to client interest in this market and it identifies market issues and trends that impact current federal contractors and vendors entering or already in the security market through FY 1997. Insight into agency requirements, regulations, and contractor perceptions are offered to help vendors plan their strategies to compete for federal security contracts.

This report on security products and services applicable to the federal government was prepared as part of INPUT's Federal Information Technology Market Program (FITMP). Reports issued through this program are designed to assist INPUT's U.S. industrial clients in planning how to satisfy future federal government needs for computer-based information systems and services. The report's findings are based on research and analyses of several sources, including:

- INPUT's Procurement Analysis Reports (PARs)
- OMB/GSA/NBS Five-Year Information Technology Plans for 1991-1996
- Past interviews with leading vendors pursuing the federal computer security market
- Past interviews with agency representatives
- An in-depth interview with representatives from the National Institute of Standards and Technology's Computer Systems Lab
- Federal agency FY 1991 and FY 1992 Information Technology Plans
- Federal reports, studies, and other secondary research sources

A
Scope

The forecast period covered in the report is FY 1992 through 1997. Agency and vendor surveys were not conducted for this report update.

For the purpose of this 1992 study, INPUT's definition of computer security encompasses the following categories of vendor products and services:

- Equipment
- Software products
- Professional services

This report supplements INPUT's previous reports on professional services. It is intended to give INPUT's clients a clearer understanding of the current status and future trends of the federal market for computer security. It also identifies the key vendors in the market, a subject of continuing interest to INPUT clients.

B
Methodology

In developing this report, INPUT used a variety of sources and methods. First, INPUT researched agency long-range plans and budget submissions for FY 1992-1997 for major programs and new initiatives involving security of sensitive systems. Based on this research, INPUT pinpointed agencies and programs that related to computer security.

INPUT reviewed its Procurement Analysis Reports (PARs—part of the Federal Information Technology Procurement Program) to develop further insight on agency activities. Many PARs cover programs that, for one reason or another, do not appear in the agency budget submissions. The PARs yield additional possibilities for further research.

INPUT also interviewed agency executives at the policy level with the National Institute of Standards and Technology (NIST) to identify current trends and issues relevant to the federal computer security market. INPUT developed a specialized questionnaire for the NIST interviews (Appendix F).

The current versions of the Federal Information Resource Management Regulations, Federal Acquisition Regulations, Defense Acquisition Regulations (changes to FAR), and relevant federal legislation and agency regulations were investigated to identify provisions that will impact computer security contracts and/or contract performance.

C
Report Organization

In addition to the introduction and appendixes, this report consists of five chapters:

- Chapter II contains an executive overview describing the major points and findings in the report.
- Chapter III provides the market forecast and describes the major market issues and trends impacting the industry.
- Chapter IV summarizes the federal agencies' requirements for computer security and the existing and planned implementation of security requirements.
- Chapter V presents vendors' perspectives on the federal computer security market.
- Chapter VI provides a sample of business opportunities for programs and initiatives in the federal market involving computer security.

Several appendixes are also provided:

- Interview Profiles
- Definitions
- Glossary of Federal Acronyms
- Policies, Regulations, and Standards
- Related INPUT Reports
- INPUT Questionnaire

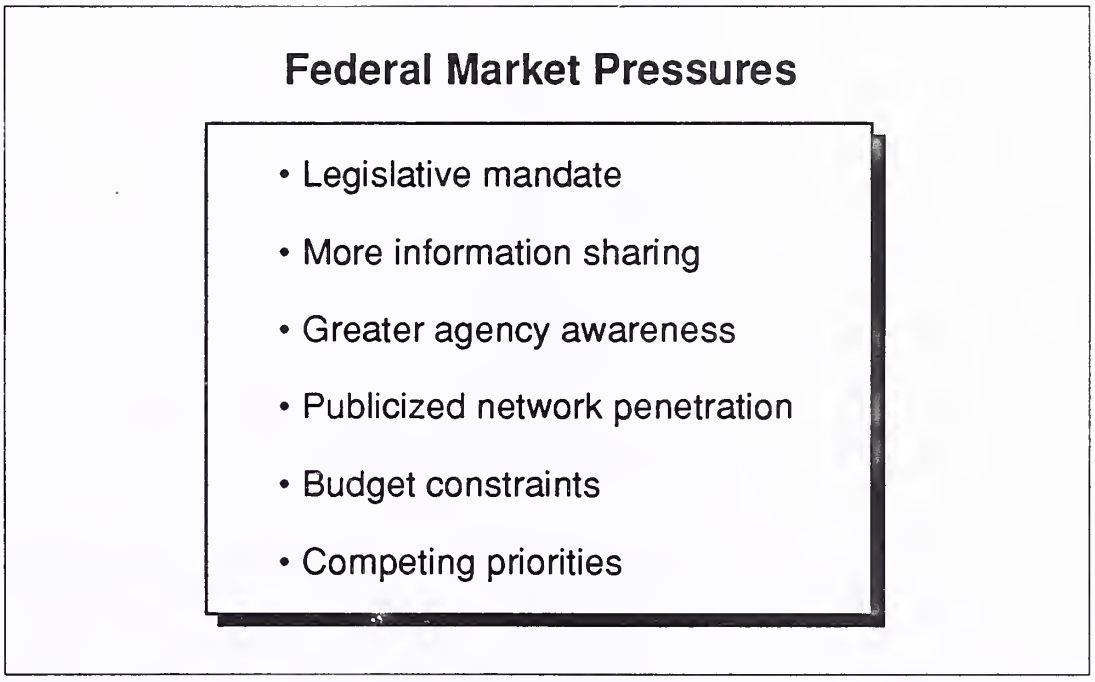
II

Executive Overview

A
Federal Market Pressures

The federal market for computer security products and services is expected to grow over the next five years. Exhibit II-1 lists some of the forces driving this growth, both in positive and negative terms.

EXHIBIT II-1



The Computer Security Act of 1987 (signed into law in early 1988) leads the list. It requires each agency to develop a computer security plan and initiate computer security training. Congress continues to encourage greater computer security. Most agencies have moved computing power to the end user and have enhanced information sharing through local- and wide-area networks, increasingly widespread use of microcomputers, and relational data base approaches to managing agency information. This

information sharing fosters compatibility and interoperability standards, leading to demands for a more open network architecture. However, the security risk increases as it becomes easier to share information over open networks.

Further, many agency executives have become increasingly aware of the need for computer security. A variety of factors are driving this increased awareness. The penetration of the NSF Internet network, which was heavily covered by the media, probably did more than anything else to increase security awareness.

On the other hand, there are also some market forces that discourage the growth of federal computer security. Continuing budget constraints are the biggest single inhibitor. Some of the oversight agencies have had their own computer security budgets cut, in part for irrelevant reasons. Individual agencies operating under constrained budgets are also trading off enhanced computer security for greater operational effectiveness. This is especially true in the Tempest equipment market, which is practically flat. Many agencies are allocating their limited resources to other, more pressing initiatives, whenever there appears to be a greater payoff.

Most agency executives and congressional decision makers do not appreciate the potential loss from security mishaps. The Internet virus did little real harm, as has been the case with most security breaches. Until major damage occurs that might involve loss of life or major property loss, few significant market changes will occur.

Despite several attempts in 1988 and 1989, Congress failed to pass any follow-up computer security legislation. This showed a reduction in congressional concern, and with it a lessening in appropriation efforts. Although the development of agency security plans represented a positive factor, the quality of those plans has to be viewed as a negative. Among other things, these plans

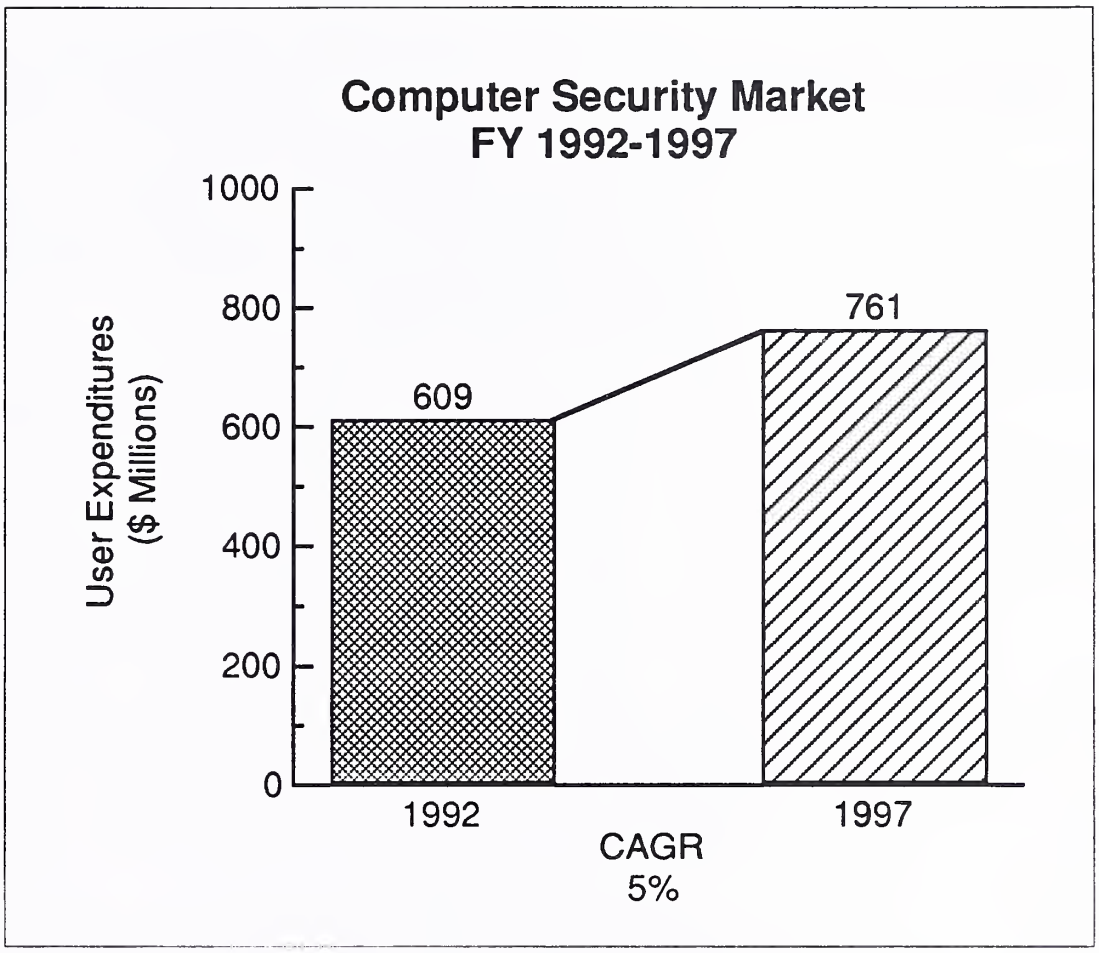
- Overlooked integrity and availability requirements
- Failed to involve user organizations
- Omitted, for the most part, network security

This suggests that, for many agencies, the planning effort became a mere paperwork exercise.

B
Market Forecast

INPUT expects that the federal computer security market will grow from $609 million in FY 1992 to $761 million FY 1997, at a compound annual growth rate (CAGR) of 5%. Exhibit II-2 displays the overall forecast.

EXHIBIT II-2



Software products will show the fastest growth rate, as agencies use them to improve security in their installed systems. The equipment market will remain fairly flat at a CAGR of only 4%, reflecting

- Reduced demand for Tempest products
- A relaxation of some Tempest standards
- Growing cost-effectiveness of Tempest technology

The market for professional services will remain flat, reflecting a saturated market for these services.

Network security consists of products such as encryption equipment and antivirus software. It is excluded from INPUT's forecast model because of the embedded nature of its processing. However, it still represents a major business opportunity in the federal market. INPUT has sized this market at approximately $417 million for FY 1992, and expects it to grow about 20% annually over the forecast period. Because of the increased use of LANs and microcomputers, this market will continue to grow at a steady rate.

C
Leading Vendors

INPUT encountered a fairly wide divergence of opinion on the identity of the leading vendors in the federal computer security market. Exhibit II-3 compares agency and vendor responses to this question.

EXHIBIT II-3

Views on Leading Computer Security Vendors

Agency Views	Vendor Views
Comsis	Digital Equipment
HFSI	AT&T
IBM	IBM

Only IBM made the top 3 of both lists. Comsis is an 8(a) firm that won a GSA contract to help agencies develop their security plans. DoD agencies think of HFSI, formerly Honeywell, in terms of the World Wide Military Command and Control System. It is interesting to note that Digital was rated first by the vendors, but was not mentioned by a single agency.

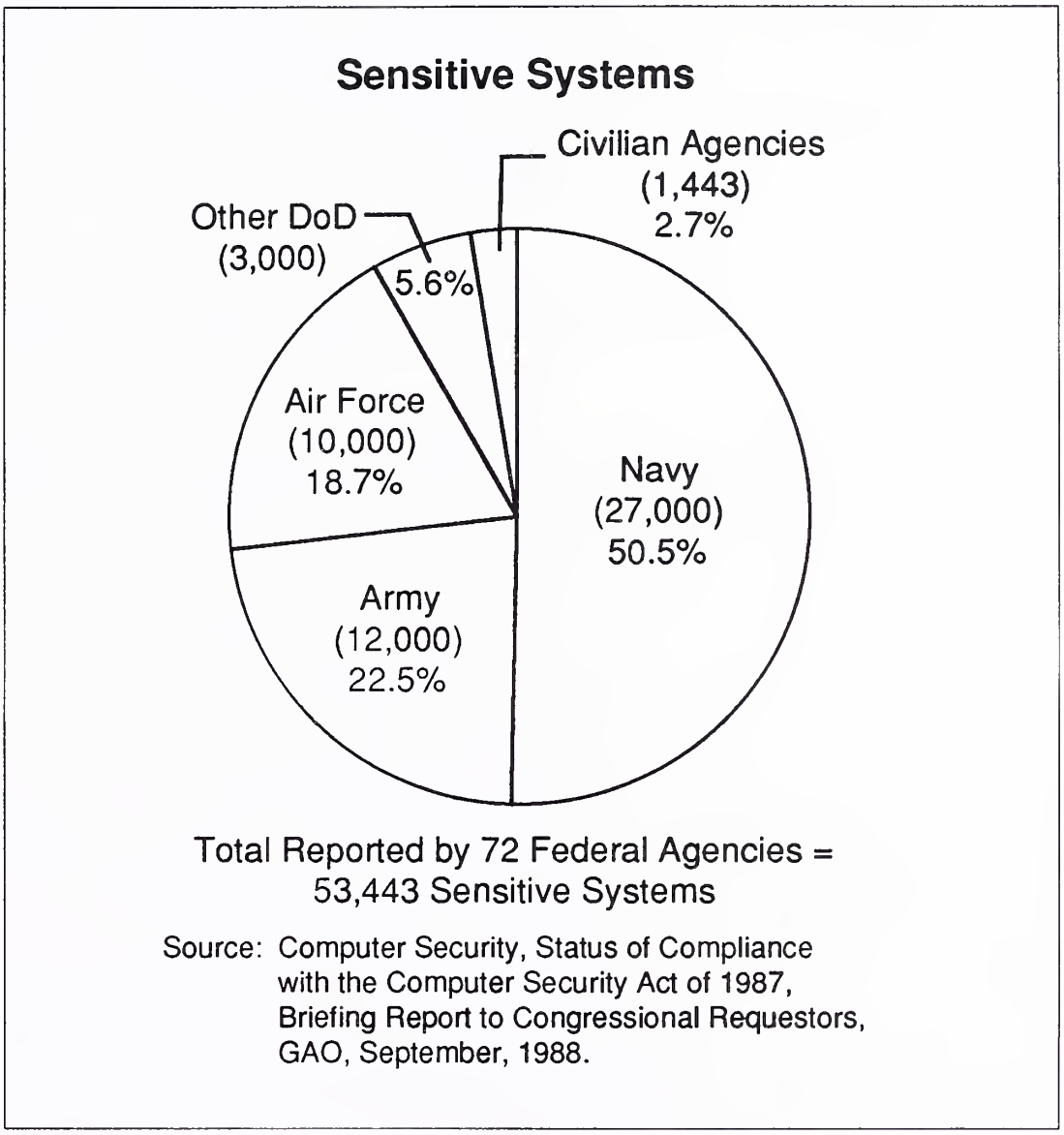
D
Sensitive System Population

In 1988, the GAO reported 53,443 sensitive systems itemized by 72 agencies responding to a survey. Exhibit II-4 summarizes the results to the survey. Two interesting findings emerge:

- More than 97% of all sensitive systems belonged to the Defense Department. This may actually overstate the proportion somewhat, due to reporting- and definition-related irregularities. It is obvious that most of the target market is in Defense. However, when the vendors were asked which agencies offer the greatest opportunities, the Treasury Department headed the list.

- More than half of all sensitive systems were listed as in the Navy. This is surprising, given the volume of work in the other military services. It may reflect, however, reporting and definition irregularities. However, it certainly suggests that vendors with limited marketing resources should concentrate on the Navy.

EXHIBIT II-4



Further research shows that many civilian agencies aggregated their systems, thus reducing the total number. Defense agencies, however, did not consolidate systems, which drove up their numbers. This suggests that vendors may pursue far more than the 53,000 systems that the GAO identified.

E

Functional Requirements

Exhibit II-5 summarizes the results of the survey of functional requirements for computer security. Most agency respondents provided more than one answer. All participants in the agency survey specified the need for network security, although it is unusual for agency respondents to agree universally on anything. This response suggests the importance agencies assign to securing their networks. INPUT has found in other surveys that agencies rely heavily on their networks.

EXHIBIT II-5

Functional Requirements for Computer Security

Requirement	Percent of Respondents*
Network Security	100
End-User Access	95
Data Security	91
Physical Security	86

*Adds to more than 100% due to multiple responses.

The other functional requirements listed in Exhibit II-6 also received high ratings. In INPUT's view, these accurately reflect agency needs in computer security. Functional safeguards to assure limited and proper access to sensitive data include encryption techniques, passwords, and multilevel security operating systems. Data security helps agencies protect the accuracy, integrity, and continuity of stored information. Physical security, often the least costly requirement, includes access to computer centers, remote processing sites, and any additional LAN or WAN sites.

F
Acquisition Methods

By a fairly sizable margin, most agency respondents stated that they prefer to use the GSA Schedule to acquire computer security products and services. Exhibit II-6 shows the results of this survey question. The schedules are most appropriate for software-related products and training tools, particularly less expensive items. However, some security-related services are available through GSA contracts, and respondents may have been including them with the schedules.

Solicitations for specific purchases and requirements contracts received almost equal ratings. There is a growing trend among agencies to use requirements contracts in a variety of areas, and this is apparently extending to computer security.

Security products are also being acquired as part of other procurements, such as Treasury's TMAC and DMAC procurements, that were cited by agency respondents. Further, most systems integration solicitations contain security requirements, included within other functional requirements.

EXHIBIT II-6

Methods of Acquisition

Method	Percent of Respondents*
GSA Schedules	85
RFP for Specific Purchase	60
RFP for Requirements Contract	55
Purchase Security Devices as Part of Other Procurements	40
Other Methods	20

*Adds to more than 100% due to multiple responses.

G
Recommendations

In providing computer security products and services to the federal government, vendors need to take a flexible approach. While there are clearly some definite needs, as in network security, likely spending remains somewhat ambiguous. If Congress continues to pressure the agencies, spending may increase slightly more than forecast, but probably not much. Vendors need to include security products as part of other offerings, such as professional services or network development and implementation.

Vendors should focus less on Tempest equipment. In past decades, Tempest equipment was the largest portion of the security market. But because of the end of the Cold War and the lessening threat from other nations, Tempest equipment is not as necessary as in the past. Professional services, software, and other security hardware will demand larger portions of the computer security market.

Many agency purchases of computer security will come through systems integration contracts, which do not focus specifically on computer security. Therefore, vendors specializing in computer security should establish teaming relationships that enable them to participate in large, complex bids.

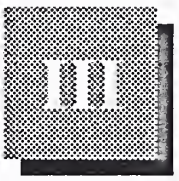
Security vendors should also develop products that accommodate the widely varied systems and equipment types in the federal market. To the extent that security products accommodate applicable federal standards, potential market penetration will increase.

Finally, vendors should train agencies and offer products for effective security management. Many agencies fall short in this area. They need to be taught how to monitor, manage, and upgrade their computer security. Also, they need to be pushed to develop contingency plans in case of security problems. Vendors who can help agencies with these management issues will have a competitive advantage.

EXHIBIT II-7

Recommendations

- Include security as part of other offerings
- Reduce focus on Tempest equipment
- Establish effective teaming arrangements
- Develop portable and interoperable products
- Train agencies in effective security management



Market Analysis and Forecast

A
Market Evaluation and Development

Computer security for the federal government focuses on protecting the confidentiality, availability, and integrity of federal information systems. It also includes assuring the accuracy and accessibility of information so that the public can be informed and agencies can discharge their duties efficiently and responsively.

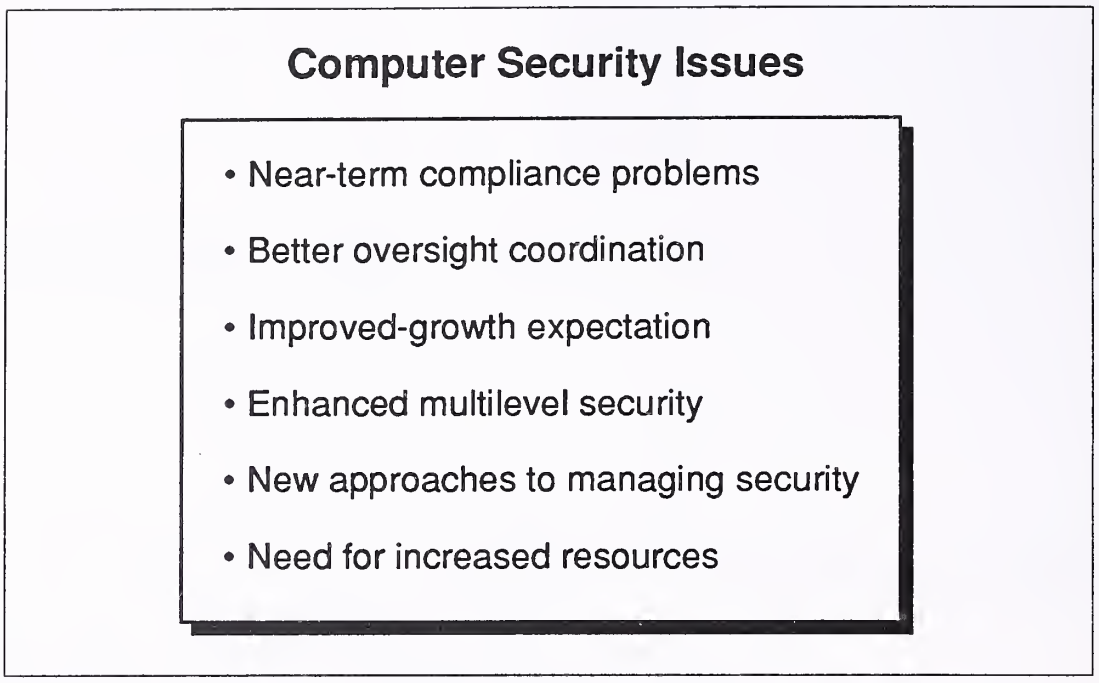
In support of federal agency missions and applications, computer security assists with the management of systems in performing the appropriate functions. Security works to protect information in the systems from unauthorized disclosure and unauthorized or inadvertent modification. It also ensures that information is available on a timely basis. However, it is important to note that in many federal systems, such as weather monitoring systems, protection from disclosure is not the primary security needed since the information is intended for widespread dissemination.

The government's management and regulation of the security of its information technology systems has a lengthy history of executive policies and legislative/regulatory initiatives. These are discussed in Section E.

Exhibit III-1 summarizes some key security issues.

Many agencies are experiencing problems with near-term compliance for computer security. For the most part, they are considering computer security when developing specifications for future systems, but retrofitting existing systems with security features is more difficult. According to a 1990 GAO report, only one of 23 agencies interviewed had instituted security measures and training required by the Computer Security Act.

EXHIBIT III-1



Better oversight coordination is needed within the agencies, as well as between agencies governing security policy. Many agencies lack emergency or contingency plans pertaining to computer security. Also, NSA, NIST, OMB, and GSA need better coordination of efforts for monitoring security compliance and standards development.

INPUT expects to see more growth in this market than in past years. As technology progresses and systems become more open and user friendly, they also become more vulnerable to security violations. Increased networking requires new approaches to managing security, especially as it relates to microcomputers. Additionally, there has been renewed interest in complying with the Computer Security Act.

INPUT also expects to see new products with enhanced multilevel security. These products will limit access of certain data to specific users in a single file. All data within the file is encoded so that it is accessible at specific levels. Two different users within the same file, network, data base, etc. have access to different sets of data.

Computer security places an additional strain on already tight agency budgets. Aware that retrofitting systems is excessively expensive, some agencies are adopting a systems life cycle approach to security. Government-wide, an increase in manpower and funding is needed for the implementation of security plans, federal employee training, and installation of security controls for government information systems.

Defense concerns about computer security led to the publication in 1983 of the *DoD Trusted Computer System Evaluation Criteria*, commonly referred to as the "Orange Book." DoD published a revised standard in 1985, with the same name and the code of DoD 5200.28-STD. The Orange Book established a series of computer security rankings, which are summarized in Exhibit III-2.

EXHIBIT III-2

Computer Security Levels

- Division A: verified protection
  - Class A1: verified design
  - Beyond Class A1: future technology
- Division B: mandatory protection
  - Class B1: labeled security protection
  - Class B2: structured protection
  - Class B3: security domains
- Division C: discretionary security protection
  - Class C1: discretionary security protection
  - Class C2: controlled access protection
- Division D: minimal protection

In evaluating federal computer security in the 1990s, vendors need to take a cautious approach to Orange Book standards. These standards may be at least partially supplanted. The European Community is taking a more global approach to developing computer security standards. It is working to develop formal standards with the International Standards Organization.

This approach appeals to many vendors, who have long complained about the length of NSA review and NSA's refusal to follow anyone else's evaluation. NSA is beginning to play a less dominant role in overall federal computer security by focusing on classified systems. NIST is emerging as a computer security authority for civilian agencies.

Despite the passage of the Computer Security Act in late 1987, relatively few agencies showed much interest in computer security. This changed at least temporarily in November, 1988, when a virus penetrated thousands of computers on Internet, an unclassified multinetwork system connecting more than 60,000 computers nationally and internationally. The interest of the press, the public, and subsequently the Congress led to still another GAO report. Federal funding contributes about $50 million annually to Internet, with most coming from the National Science Foundation (NSF) and DoD's Advanced Research Projects Agency (DARPA). GAO identified several Internet vulnerabilities:

- No Internet security focal point
- Security weaknesses at host sites
- Weak procedures for correcting software holes

A college student was convicted for his involvement in the virus. As might be expected, the Congress expressed concern over the developments, but did nothing. Section E covers recent legislative attempts.

Early in 1989, a team of security experts began reviewing the security plans required from each agency by the Computer Security Act. Personnel from the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) comprised the team. Initially, the civil agencies submitted 1,700 plans, while the defense agencies submitted only three plans. This apparently resulted from a misunderstanding on jurisdiction. Subsequently, in August 1989, Defense agencies submitted 29,000 plans. Although the team obviously could not review all these plans, it did provide 450 sets of comments. In general, the team identified the following problems with the plans:

- Integrity and availability requirements were overlooked.
- Confidentiality issues were overly stressed.
- User organizations apparently did not participate in the development of the plans.
- State and local government organizations with federal funding, as well as federally funded contractors, failed to provide any plans.
- Few plans addressed network security.
- Few plans covered microcomputers adequately.

Despite these problems, NIST cited some benefits to the overall process:

- Many federal agencies performed security planning for the first time.

- Other agencies reevaluated their security planning practices.
- Most of the review team's comments were well-received by the agencies.
- Despite fears to the contrary, NIST and NSA worked well together on the review effort.

In May, 1990, GAO published a brief report on the security planning process. As might be expected, GAO had little positive to say:

- The security plans had limited impact on agency computer security programs. Only one of 23 reviewed federal agencies had instituted security measures and training.
- The plans lacked adequate information to serve as effective management tools.
- Managers had insufficient time to prepare the plans.
- Guidance was sometimes unclear and misinterpreted by agencies.
- Agencies have not implemented most planned security controls.
- NIST/NSA review and feedback was general and of limited use to agencies.

GAO did add that new OMB guidance on security planning may assist future agency planning efforts. However, the results suggest that vendors need to develop a strong marketing effort in order to create greater demand among the agencies.

Also in 1990, the Computer System Security and Privacy Advisory Board issued a number of reports evaluating agencies' ADP security material weaknesses. A summary of this report identified agencies with inadequate security programs or policies, and agencies with inadequate or no contingency plans. These agencies are listed in Exhibit III-3.

EXHIBIT III-3

Agencies with ADP Security Weaknesses

Inadequate Security Programs or Policies	Inadequate or No Contingency Plans
Veterans Affairs	Veterans Affairs
Treasury	Treasury
Health and Human Services	State
Education	Education
Agriculture	Federal Communications Commission
Commerce	Securities and Exchange Commission
Defense (Joint Staff)	Agriculture
Justice	Defense
Securities and Exchange Commission	Interior
FBI	Justice
	Marshals Service
	Drug Enforcement Agency

In May 1991, the National Computer Security Center (NCSC) published a document defining its criteria for evaluating the security of relational data base systems (RDBMS). The Trusted Database Management System Interpretation (TDI), or Lavender Book, defines how manufacturers can produce RDBMS that meet computer security criteria established by NSA's Orange Book. This is a major step toward the availability of preapproved multilevel secure data bases to federal agencies. Companies with RDBMS products currently under evaluation by NCSC are Informix, Oracle, and Sybase.

B
Market Structure

The federal computer security market, like many other specialized areas, may be broken out into various distinct segments, as follows:

- Computer security equipment includes processors and peripheral equipment that are Tempest shielded (i.e., electronic or electromechanical emanations are blocked), as well as processor-based equipment used in the protection of computer systems. For the purposes of this report, this category does not include electronic locking systems, fire protection systems, or encryption devices. General-purpose computer systems that have been modified are included, as well as Tempest-protected CD ROM products, such as those from Memory Storage Devices. This category does not include electronic access control devices, such as the Retinal Scan device from Eye Dentify, Inc.

- Computer security software products include any commercially available product whose primary function is to enhance the security system. It does not include general-purpose operating systems that incorporate standard security features. However, software specifically aimed at security is included. For example, the Sun OS MLS, a multilevel secure UNIX operating system, is included, as are the various antivirus products, such as N-Vir Assassin for the Macintosh or Vi-Spy for the IBM PS/2. Software products supporting communications security, such as Verdix's VIbus interface and 3COM's upgraded security features on its network control servers, are also included, as are mainframe products such as IBM's RACF and CA's ACF II.

- Professional services includes INPUT's four delivery submodes:

- Consulting services includes feasibility studies, requirements analyses, risk analyses, security plans, and system audits. Many agencies used consultants to assist them in writing the new plans required by the Computer Security Act. However, this appears to have been a one-time opportunity, since NIST is not expected to require updates.

- Education and training are important components of this market, since the Act requires that all federal employees with access to computer files receive training. There are several companies currently supplying computer security training. Further, the Office of Personnel Management issued a final ruling on the Computer Security Act in 1991 that requires agencies to train federal users and managers who use computer systems to process sensitive information.

- Software development relates to custom-tailored efforts to enhance security at a particular client, location, or system. Modifications to standard products to suit a particular client's security needs also fall into this category.

The federal computer security market includes other products and services that operate in classified environments (for example, Unisys' Blacker system, supporting network security, and the Xerox Encryption Unit). Software to facilitate NSA code breaking might also be considered a computing security product.

Information on acquiring these products is classified, making it impossible to develop market sizing information. Accordingly, INPUT has not included them in this market structure or in the market forecast provided in the next section. However, when general information on these products and services is publicly available, INPUT has included that information in this report.

1. Perceived Market Differences

Agency and industry respondents, in a past survey, were asked their opinions on the differences between the defense and civilian agency markets for computer security products and services. Exhibit III-4 compares the agency and vendor perceptions obtained. In general, the responses present different perspectives—the agencies as users and the vendors as suppliers.

The agency respondents directed some of their comments to the more rapid growth in the civilian market. In their opinion, the civilian market is also subjected to stronger influence from the commercial industries. Several respondents pointed to the Treasury Department as a prime example. They expect computer security to be emphasized more at civilian agencies that address financial and law enforcement matters. Less emphasis is expected at agencies with scientific missions, since they require shared technical information to be widely accessible.

EXHIBIT III-4

Perceived Differences— Civilian and Defense Markets

Agency Respondents	Rank*	Industry Respondents
Market increasing more rapidly in civilian sector.	1	Defense market subject to stricter standards and requirements.
More defense-oriented products available.	2	Employees at civilian agencies have less security training and awareness.
Defense agencies and State Department most active in establishing security requirements.	3	Differences in volume of classified data (DoD greater)
Banking and insurance industry security will impact civilian agencies—especially Treasury Department.	4	Increased opportunities for custom solutions in defense agencies.

*Rank based on frequency of mention by respondents.

From the vendors' perspective, the defense agencies appear to be more likely potential targets for their products and services, since many vendors are already well-known at some agencies and are more familiar with the agencies' information systems. The civilian agencies are viewed as a growing market for products, due to the additional security requirements the agencies have added to comply with government legislation. Further, some security agencies also manage classified information.

The majority of industry respondents noted that there are more numerous and stricter requirements and standards imposed upon the defense agencies that are not applicable to the civilian agencies. These requirements and standards in turn increase vendor opportunities to provide customized hardware and software for computer security installations.

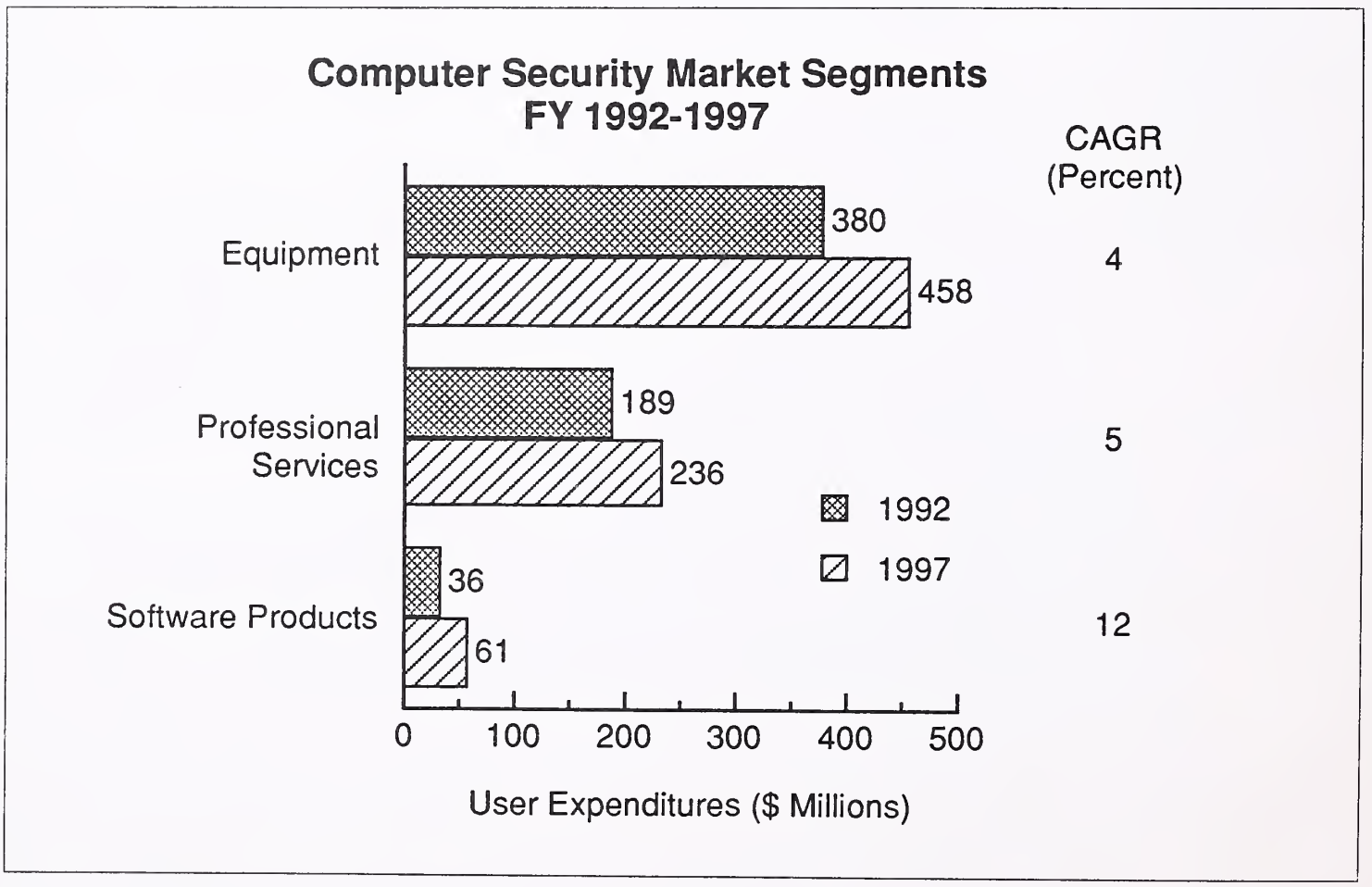
Another notable difference from the vendors' point of view was the greater level of awareness and training at defense agencies. At the civilian agencies there is now greater need for training to bring employees up to the level of awareness required by the Computer Security Act. This training is already under way in many agencies.

C
Market Forecast

The federal computer security market will grow from $609 million in FY 1992 to $761 million in FY 1997, at a CAGR of 5%. With inflation factors taken into account, this could be considered a declining market. But with recent attention focusing on computer security problems within agencies, there is an improved-growth expectation in this market.

As described in the previous section, this market includes the equipment, software products, and professional services that operate in an unclassified environment. The forecast for the subsegments of this market is shown in Exhibit III-5. With classified applications added, the market size would probably increase sharply. However, since such information is not publicly available, it is omitted from this forecast.

EXHIBIT III-5



In part, the overall federal IT market is determining the viability of the federal computer security market. The extent to which agency program managers include security requirements in their solicitations will drive both market size and complexity. The Computer Security Act defined sensitive information as that whose "loss, misuse, or unauthorized access to or modification...could adversely affect the national interest or the conduct of federal programs or the privacy to which individuals are entitled under [The Privacy Act]."

Therefore, solicitations that place a high premium on confidentiality, integrity, and availability will spur the need for products and services. The Computer Security Act also requires annual security reviews. If OMB enforces this requirement, it will lead to significant opportunities for professional services firms. On the other hand, if these reviews become a paperwork exercise, most agencies will apply few resources to the effort.

Although computer viruses receive much media attention, NIST has stated that they are not the major problem. Rather, NIST stresses the need for security management and oversight. If this view spreads throughout the government, professional services opportunities might grow at the expense of software products. This counters the overall federal IT trend, which currently favors software products over professional services.

In defining the federal computer security market, it is helpful to examine market issues among various market segments:

- Processing Services: Computer security takes several forms in contractor-operated agency processing environments, both government-owned and contractor-owned. Two NASA COCO facilities, at Goddard Space Flight Center and Ames Research Center, have established Computer Security Incident Response teams. The FBI has established a Library Awareness Program to monitor circulation, on-line data base, and inter- and intralibrary programs, to ensure data integrity.

- Professional Services: The federal government will spend ample sums on professional services support to help meet its computer security needs. First, as already pointed out, the Computer Security Act requires appropriate training of appropriate personnel. Although OPM has been very active in this area, various private providers are also providing computer security training to federal personnel. Consulting support will continue to be needed for security evaluations and audits, as well as for upgrading computer security measures. However, if the agencies are not required to submit updated security plans, the volume of planning opportunities will likely disappear. Custom software development will also play an important role. For example, IRS hopes to achieve C2-level security for its Tax System Modernization program. Unique software development will be needed to achieve that goal.

- Software Products: The growing availability and functionality of software products, especially in the area of network security, are spurring this market. For example, it has been reported that the market for secure UNIX products has grown sharply as a result of the Internet virus. The Small Business Administration is using software products to define its computer security needs. SBA developed its "BASIC" software procedures in conjunction with the Federal Judiciary Center and the Department of Veterans Affairs. Despite the fact that the software itself does not actually protect anything, it still needs to be included in the software products segment of the federal computer security market, since its usefulness and salability depends on that market.

- Computer Equipment: As indicated in the previous section, specialized computer equipment, including Tempest-shielded equipment, forms the primary (in terms of funding) component of the federal computer security market. Much of this equipment is listed on the Preferred Products List (PPL) developed and maintained by NSA. However, the PPL has been criticized as being too lax in enforcement of its standards. In response, NSA is moving toward more exacting standards with its Endorsed Tempest Products List (ETPL). An even more exacting list, the Potential ETPL, is also under consideration. These lists, plus some relaxation in Tempest standards, have led to some market confusion. The DoD budget cuts are aggravating this problem.

- Telecommunications: The network security market was discussed briefly in the preceding section. Although from a technical standpoint LANs may not involve telecommunications, INPUT includes them in the telecommunications category because of the similar functions. LAN use in the federal market has grown considerably, increasing the potential for viruses. This opens the market to virus protection software and products that limit accessibility.

- Electronic Data Interchange (EDI): As reported in INPUT's *Federal EDI Market* report, budget constraints are encouraging greater use of EDI in the federal market. As EDI becomes more commonplace, the potential for security violations increases, which concerns both agencies and vendors. In previous agency and vendor surveys, INPUT asked about the impact of security requirements on EDI and CALS. Exhibits III-6 through III-9 summarize the results. It should be noted that most of the responses for EDI also applied to CALS. These responses suggest some limited concern on the part of agencies and vendors.

EXHIBIT III-6

Agency Views of Security Regulations' Effect on EDI Initiatives

- Delay of approved classification
- Privacy/data integrity requirements
- Additional complexity of initiatives
- Additional security required of software
- None

EXHIBIT III-7

Vendor Views of Security Regulations' Effect on EDI Initiatives

- Increased costs
- Need to integrate with other systems
- Need for improved NIST standards
- Regulations not yet solving EDI security problems

EXHIBIT III-8

Agency Views of Security Regulations' Effect on CALS Initiatives

- Increased software security capabilities
- Insufficient guidance on CALS standards
- Delay of approved classification
- Additional complexity of initiatives
- None

EXHIBIT III-9

Vendor Views of Security Regulations' Effect on CALS Initiatives

- Increased costs
- Need to integrate with other systems
- Risky concentration of sensitive data
- Additional restrictions being imposed
- Need to insure data integrity
- Need to increase priority of CALS security

According to NIST, the past jurisdictional disputes between itself and NSA have been resolved. The problem originally surfaced with the passage of the Computer Security Act, which gave broad powers to NIST, some of which formerly belonged to NSA. The dispute nearly disappeared in 1989, when the two agencies worked very effectively together in reviewing agency security plans. However, problems resurfaced as congressional pressure increased to finish the development of governmentwide computer security standards.

In the summer of 1991, the two agencies were still bickering over a set of standards. NSA wanted to emphasize higher-level security measures for highly sensitive data, while NIST pressed for measures to protect less sensitive data. NSA argued that standardizing technologies for common manufacture and use would allow them to fall into the hands of foreign enemies.

However, in early 1992, NIST and NSA reached an agreement on how to test new computer security products. Under the new arrangement, NIST will test lower-level security products, while NSA will continue to evaluate products intended for use in protecting national security information. This relieves NSA of some testing responsibility.

NIST and NSA also released a draft of Federal Criteria for Trusted Systems Technology intended to update the Orange Book. Hopefully, this is a step toward releasing jointly developed federal computer security standards, due to be published as Federal Information Processing Standards (FIPS).

NIST continues to play the primary role in computer security policy in civilian agencies, while NSA remains responsible for defense-related and classified computer security.

INPUT's market forecast is lower than other estimates reported in the press. For example, another market analyst estimated that procurement of Tempest equipment, with added secure telephones, could rise to more than $1 billion by 1994. Apparently, this forecast is based primarily on past sales patterns, relaxation in some agency Tempest requirements, and growing recognition of the importance of Tempest products in various categories.

Unfortunately, the Defense IRM budget cuts of nearly $600 million in FY 1990 included initiatives requiring Tempest-approved computers and equipment. Though cuts were widely anticipated, the magnitude exceeded most forecasts. These cuts have tended to reduce demands for Tempest equipment. Instead of automatically including Tempest requirements, many agency program managers, facing budget constraints, now question the need for Tempest shielding and are seeking ways to avoid it.

The growing cost-effectiveness of Tempest technology has also dampened market growth. An analysis of the history of Tempest-approved computer prices shows that most systems now cost only 50%-75% more than comparable non-shielded systems. As a result, when protection is required, agencies can often obtain it more economically than was possible several years ago.

Similarly, spending on software products and professional services will be fairly constrained. However, if an expensive or life-threatening security violation should occur, the situation could change drastically. Congress would be expected to recognize the problem and fund accordingly.

Network security also represents a significant business opportunity in the federal market. Strictly speaking, this market is outside INPUT's model, since it consists of data encryption and other equipment usually excluded from INPUT's categories. However, numerous software products, such as the software controls on 3COM's network servers and Verdix's VIbus interface, are included in INPUT's software products forecast.

INPUT estimates that the current federal market for network security products and services is $417 million, and it is expected to grow by 20% annually over the next few years. INPUT expects the civilian share to increase with corresponding cuts in Defense. The press has reported market estimates ranging from $341 million to more than $2 billion. INPUT's estimate falls on the low side of that range, based on current and expected future Defense budget cuts.

This market could increase at a faster pace, however, if the vulnerability of public switched network systems increases. There have been rumors of AT&T losing control of central switches, and of the Secret Service looking into it. If this is true, it may give way to a new federal initiative on enhanced security of public communications systems.

D
Federal Market Pressures

There are competing market pressures driving this market. Exhibit III-10 lists the major pressures. On the positive side, the Computer Security Act of 1987 (signed in early 1988) required that each agency develop a computer security plan. However, the requirement for computer security training probably did more to encourage greater understanding and appreciation of the problem among federal officials.

As in the private sector, most federal agencies have moved computing power to end users through microcomputers, workstations, and local-area networks (LANs). Many agencies require greater sharing of information, which fosters compatibility and interoperability standards. This leads to requirements for greater ease of use. Agencies put a premium on software features that reduce human effort and error. However, these same features tend to enhance the risk of security violations. The systems' ease of use encourages ease of abuse. The open network architecture that many agencies require often includes the mandatory use of the Government Open System Interconnect Profile (GOSIP) standard. All of these information sharing initiatives represent a threat to computer security and safety.

EXHIBIT III-10

Federal Computer Security Market Pressures

- Encouraging computer security expenditures
  - Legislative mandate
  - Greater end-user computing
  - More information sharing
  - Open network architecture
  - Greater agency awareness
  - Publicized network penetration
  - Increased number of incidences
  - Dedicated staffs
- Discouraging computer security expenditures
  - Budget constraints
  - Competing priorities
  - Limited actual harm
  - No follow-up legislation
  - Poor planning effort

The Internet virus in late 1988 served to heighten agencies' awareness of their vulnerabilities. The virus apparently entered the network's UNIX operating system through a hole in the electronic mail system. It then shut down other operations and sent copies of itself to other computers on the network. It appears that no lasting harm was done. Lasting harm may have actually spurred the federal computer security market to higher funding levels. At any rate, the incident received (and continues to receive) great notoriety in the media, thus increasing an appreciation of the importance of computer security.

Microcomputer viruses seem to be on the rise and are costing agencies large sums of money and labor to correct. In October 1991, an epidemic of microcomputer viruses at the Commerce Department forced employees to spend nearly 200 hours on recovery work.

Finally, on the positive side, both the NIST and the NSA have staffs dedicated to computer security. To the surprise of some federal pundits, these staffs worked well together in reviewing the agency plans. NIST personnel, in particular, frequently speak at agency and commercial conferences on the importance of computer security in the federal government.

As indicated in Exhibit III-10, there are also some market pressures that discourage growth of the federal computer security market. Budget constraints account for by far the strongest restraint. Agencies rarely receive funds specifically for computer security. These funds are supposed to be part of overall funding for system management, but agencies find it very difficult to reallocate these funds. Also, computer security must compete with new program funding. Rarely is the funding for traditional programs cut in order to fund computer security efforts.

On a more global level, many agencies, especially defense agencies, are currently suffering budgetary shortfalls. Individual programs are being cut and, in some cases, employees are being laid off. In the absence of tangible evidence to the contrary, it is difficult to see an immediate payoff to computer security. In most agencies, computer security spending is being reduced to permit emphasis of higher-priority projects.

As pointed out above, the Internet virus did little real harm. This has generally been the case with most security breaches. Until apparent major damage occurs, few significant changes will occur. To consider a worst case scenario: Suppose a virus entered the FAA's Air Traffic Control System, precipitating a mid-air collision. If such a horrible event occurred, Congress would likely move quickly to improve federal computer security. However, until some really serious crisis occurs, politics as usual will likely control federal computer security. The failed attempts at follow-up legislation, discussed in detail in section E, show the lack of any congressional sense of urgency.

Although the development of agency security plans represented a positive factor, the quality of those plans has to be viewed as negative. Some of these weaknesses were discussed in Section A. Since NIST does not intend to require a second submission, many agencies will not have usable plans, at least for the foreseeable future.

E

Laws, Regulations and Policies

The federal government has taken a series of steps to enhance computer security:

1978 - Issuance of Transmittal Memorandum to OMB Circular No. A-71 (which was effective March, 1965). The memo promulgates policy and responsibilities for the development and implementation of computer security programs by executive branch departments and agencies.

1985 - Issuance of OMB Circular No A-130. The circular contains the OMB guidance relevant to security in the development of automated information systems. A-130 is an omnibus circular intended to summarize OMB guidance across all aspects of information systems. It rescinds OMB Circular No. A-71.

1985 - NSA issued the *Trusted Computer Systems Evaluation Criteria* or Orange Book.

1988 - Computer Security Act of 1987, signed into law in January 1988. (P.L. 100-235). The Act calls for development of security standards, establishment of security plans, and implementation of a comprehensive training and awareness program for all employees involved with federal computer systems containing sensitive information.

1989 - OMB issued guidance for preparation of security plans for computer systems containing sensitive information in order to assist agencies in preparing their computer security plans.

1991 - NSCS, part of NSA, issued the *Trusted Database Management System Interpretation* or Lavendar Book. This document describes how NSCS will evaluate secure relational data base management systems (RDBMS).

1991 - OPM issued a final rule on training as mandated by the Computer Security Act. The rule follows two years of interim guidance. The rule states that all government employees who use computers for processing sensitive information must undergo some form of security training. OPM defined the types of training required for employees in different categories. Agency heads, not OPM officials, are responsible for seeing that employees receive adequate instruction.

Additionally, the General Accounting Office (GAO) issued more than 40 reports between 1976 and 1988 on computer security. Most of these reports criticized agencies for having operating systems that are highly vulnerable to both internal and external threats. The GAO reports cited both personnel and systemic problems that lead to breaches in agency security.

These reports were supplemented in the early 1980s by additional studies performed by:

- The American Institute of Certified Public Accountants
- The American Bar Association
- The President's Council on Integrity and Efficiency (which reviewed ten federal centers)

These studies increased agency awareness and understanding of the growing security problem. Subsequent testimony in 1985 by GAO and other officials further highlighted the federal security problem and helped lead to new security legislation. Unfortunately, none of the reports told agencies how to secure the necessary resources to improve their computer security.

The growth of end-user computing in the federal market serves to aggravate the computer security problem. The microcomputer has drastically altered the way information is created, stored, and used. The networks that tie these microcomputers together increase the opportunities for computer hackers to penetrate restricted systems. The networks also increase the risk of computer viruses disrupting government systems. Although these networks are often indispensable to the conduct of government business, they also increase the government's vulnerability.

Following the Watergate scandals of the early 1970s, Congress mandated a physical break in the transmission of personal tax information. Thus the IRS was inhibited in its networking efforts. The Tax System Modernization program will address this problem and contain security specifications for the individual procurements involved in this program.

Congress has the difficult task of enacting laws to combat computer security violations but yet not restrict access to data that should be distributed and shared among federal system users. It also faces the challenge of keeping a balance among the various federal agencies that promulgate regulations, standards, and protect the national security. Legislators, in their enactment of the Computer Security Act of 1987 (P.L. 100-235), finally succeeded in reaching a compromise regarding the roles of NIST and NSA with respect to providing guidance and control of computer security for civilian agencies.

Prior to the passage of P.L. 100-235 the NSA, which is part of the Defense Department, was authorized under National Security Directive 145 to oversee all federal computer security standards and training. NIST and NSA developed a Memorandum of Understanding (MOU) in order to work cooperatively in carrying out their responsibilities under the Computer Security Act of 1987. The MOU established the following agreement between the two agencies:

- It recognizes NIST's responsibilities for developing security standards for sensitive unclassified (non-national security) systems.
- NIST will draw upon NSA's expertise where appropriate.
- NIST will recognize trusted system criteria.
- The MOU establishes a technical working group to resolve issues.
- The MOU directs the agencies to exchange working papers.

Together, the MOU and the Computer Security Act resulted in giving responsibility for security standards to the National Institute of Standards and Technology, a civilian agency, and having the National Security Agency, a defense agency, play more of an advisory role for computer security of sensitive data.

The Computer Security Act of 1987 (P.L. 100-235), as enacted on January 8, 1988 requires specific computer security measures to be taken by federal agencies. These include:

1. Identifying computer systems that contain sensitive information

2. Establishing a plan for security and privacy of each federal computer system identified. Plans were to be submitted to NIST and NSA for advice and comments.

3. Providing mandatory periodic training in computer security awareness and accepted computer security practices for employees involved in each computer system

Congress continues to work on legislation and revision of bills in the areas of anti-virus, hacker prevention, privacy, and computer fraud. It is predicted that future legislation will be enacted to tighten the punishment for computer crimes as a deterrent to potential hackers.

In 1989, Representative Tom McMillen of Maryland introduced the Computer Protection Act (H.R.287) to broaden the scope of computer-related activities deemed as wrongful acts to computer systems and therefore subject to jail punishments. Representative Wally Herger of Califor-

nia proposed the Virus Eradication Act (H.R.55), which was the first legislative bill introduced to deal specifically with computer damage induced by a virus. Both of these bills died at the end of the 1990 congressional year.

Currently, there is a bill on the 1992 Senate calendar called the Computer Abuse Amendments Act (Senate Bill 13-22). This bill, if enacted, would clarify and strengthen criminal laws against intentional transmission of destructive computer programs or codes, and provide a civil remedy in certain cases.

Section IV-D of this report provides a list of possible future legislation and regulations regarding computer security as predicted by NIST.

There have been several other pieces of legislation over the past 20 years that relate in some way to computer security:

- The Electronic Communications Privacy Act of 1986 protects against unauthorized interception of electronic communication, updating the 1968 voice-oriented wire tap law.
- The Electronic Funds Transfer Act of 1978 establishes criminal penalties for computer system stealing through a fraudulent transfer of funds.
- The Privacy Act of 1974 establishes criminal penalties for transferring personal information from a government data base, except under specific authorization.

F
Key Federal Agencies

In addition to the Congress, many other agencies play an active role in computer security. This section discusses the activities of some of these agencies.

1. General Services Administration (GSA)

The General Services Administration (GSA) plays a rather small role in the regulation of computer security. It is the responsibility of the GSA to issue policies and regulations for the following areas:

1. The physical security of computer rooms consistent with the standards and guidelines issued by NIST

2. Agency procurement requests for automated data processing equipment, software, and related services to include security requirements

3. Procurements made by GSA to meet the security requirements established by the user agency

The Federal Information Management Regulation (FIRMR) issued by GSA provides guidance for the acquisition and management of information resources. FIRMR guidance in 41 Code of Federal Regulations, Chapter 201 includes security for information systems under development. The automated information system development and management requirements in OMB Circular A-130 and the FIRMR are similar. For example, the FIRMR requires that federal agencies establish an adequate security program "to ensure automated information integrity; i.e., a security program that

a. Ensures that under all conditions, sensitive data is safeguarded from disclosure and protected from unauthorized modification or destruction,

b. Provides for operational reliability of ADP and telecommunications systems, and

c. Provides asset integrity for prevention of loss from natural hazards, fire, etc."

In addition, GSA's Office of Technical Assistance (OTA) has published a guideline entitled "Information Technology Installation Security."

2. Office of Management and Budget (OMB)

Under the training provisions of the Computer Security Act of 1987, OMB is directed to issue regulations prescribing the procedures and scope of the training to be provided to federal civilian employees. OMB is also to issue regulations indicating the manner in which training is to be carried out.

The training regulation OMB issued in 1988 focused on employee awareness of system vulnerabilities and risks. Federal employee training is to be a continual process at agencies. According to OMB, training will include non-classroom methods, such as videos and manuals.

Also in 1988, OMB published guidelines for agencies to use in preparing computer security plans. The OMB guidelines require agencies to document security awareness and training programs for their major application and support systems.

Additional security guidance from OMB is available to agencies in OMB Circular No. A-130. Under this circular, OMB is authorized to review agencies' policies, practices, and programs pertaining to the security, protection, sharing, and disclosure of information, in order to ensure compliance with the Privacy Act and other related statutes.

Although not directed solely at security practices, Circular A-130 contains agency responsibilities and practices that must be considered during system development in the area of information security. Specifically, OMB Circular A-130 states that agencies shall assure the following:

1. That automatic information systems operate effectively and accurately

2. That these systems incorporate appropriate technical, personnel, administrative, environmental, and telecommunications security controls

3. That the continuity of operations of information systems that support critical or sensitive agency functions be maintained

In 1991, OMB required agencies to include details of their computer security programs in their annual five-year IRM plan submissions. The new reporting requirements were part of OMB's 1991 bulletin on IRM planning. OMB officials said the new report format will help them track agency progress in improving security, evaluating IRM priorities, and reducing paperwork burdens on the public.

Under the new bulletin, agencies were required to provide a summary of the security plans they submitted to NIST in 1989. They also had to report on their emergency, backup and contingency plans.

OMB also plans to revamp its method of evaluating agency computer security programs. Recently, OMB stated it would discontinue its agency visits. It plans to develop another oversight mechanism, but it has not yet decided on a new system.

3. National Security Agency (NSA)

The National Security Agency was established by presidential directive in 1952 as a separately organized agency within the Department of Defense. NSA was charged with the mission of computer security under a 1984 presidential directive. The agency has the following responsibilities:

- Prescribing certain security principles, doctrines, and procedures for the U.S. government

- Organizing and coordinating the research and engineering activities of the federal government in support of the agency's assigned security mission

- Operating the National Computer Security Center (NCSC)

- Conducting security product evaluations/certifications (Evaluated Products List)

As noted earlier, NSA and NIST entered into a Memorandum of Understanding regarding the security of sensitive data. The Computer Security Act further specified that the technical advice and assistance of the National Security Agency shall be called upon where appropriate. NSA and NIST jointly reviewed the thousands of computer plans from the federal agencies. The plans were returned to the agencies along with comments and suggestions.

NSA's influence on the federal computer security market is most visible through its establishment of categories for levels of security (A to D) for systems as defined in the DoD Trusted Computer System Evaluation Criteria (the "Orange Book"). The National Computer Security Center evaluates and certifies computer systems according to seven levels of security. These were summarized in Section A; Appendix D describes each level in a brief narrative.

The federal agencies are striving to achieve the C2 level by 1992 as called for in Defense Directive 5200.28. Vendors such as Digital, Unisys, IBM, Hewlett-Packard, and Wang are offering products at the C2 level with optional upgrades to B1 and A1 for some products. Industry has hardware, software, dial-back modems, and encryption devices in the federal marketplace that have already passed Orange Book criteria for testing. This process can take several years, depending on the capabilities and complexity of the security product. Although no requirements exist for public key crypto, INPUT expects NSA to foster a digital signal standard. NSA is working with industry to strengthen vendors' understanding of the DoD security standards, features, and procedures for obtaining ratings for secure systems. The aim is to achieve improved consistency in products.

4. National Institute of Standards and Technology (NIST)

NIST (formerly the National Bureau of Standards) is an operating unit of the Department of Commerce. The agency's computer security mission is to:

- Develop and maintain security standards
- Assist federal agencies by providing advice and guidance in the use of standards
- Assist other agencies in specific systems development efforts
- Assist the private sector in using standards
- Conduct computer security-related research and studies

These responsibilities are reinforced by the Computer Security Act of 1987.

NIST, together with NSA, established computer security standards for civilian agencies and reviewed the computer security plans submitted by federal agencies. From NIST's perspective, the reviews identified weaknesses in agency awareness and training for security. Furthermore, NIST—in conjunction with DoD, Justice, and NSA—coordinates agency responses to computer security incidents and maintains a clearinghouse for security issues.

The National Computer Systems Laboratory operates under the direction of NIST to conduct research and be a liaison with industry. Exhibit III-11 is an organizational chart from the Laboratory. According to the Associate Director for NCSL, Lynn McNulty, the organization is concerned with a variety of security issues, including integrating security with the utilization of GOSIP and developing protection for networks and operating systems. Along with NSA, NIST conducts agency visits to investigate compliance with security requirements.

During 1989, NIST formed a twelve-member Computer System Security and Privacy Advisory Board within the Department of Commerce. The Board's Chairman is James H. Burrows, director of NIST's Computer Laboratory. The duties of the Board according to the Computer Security Act are as follows:

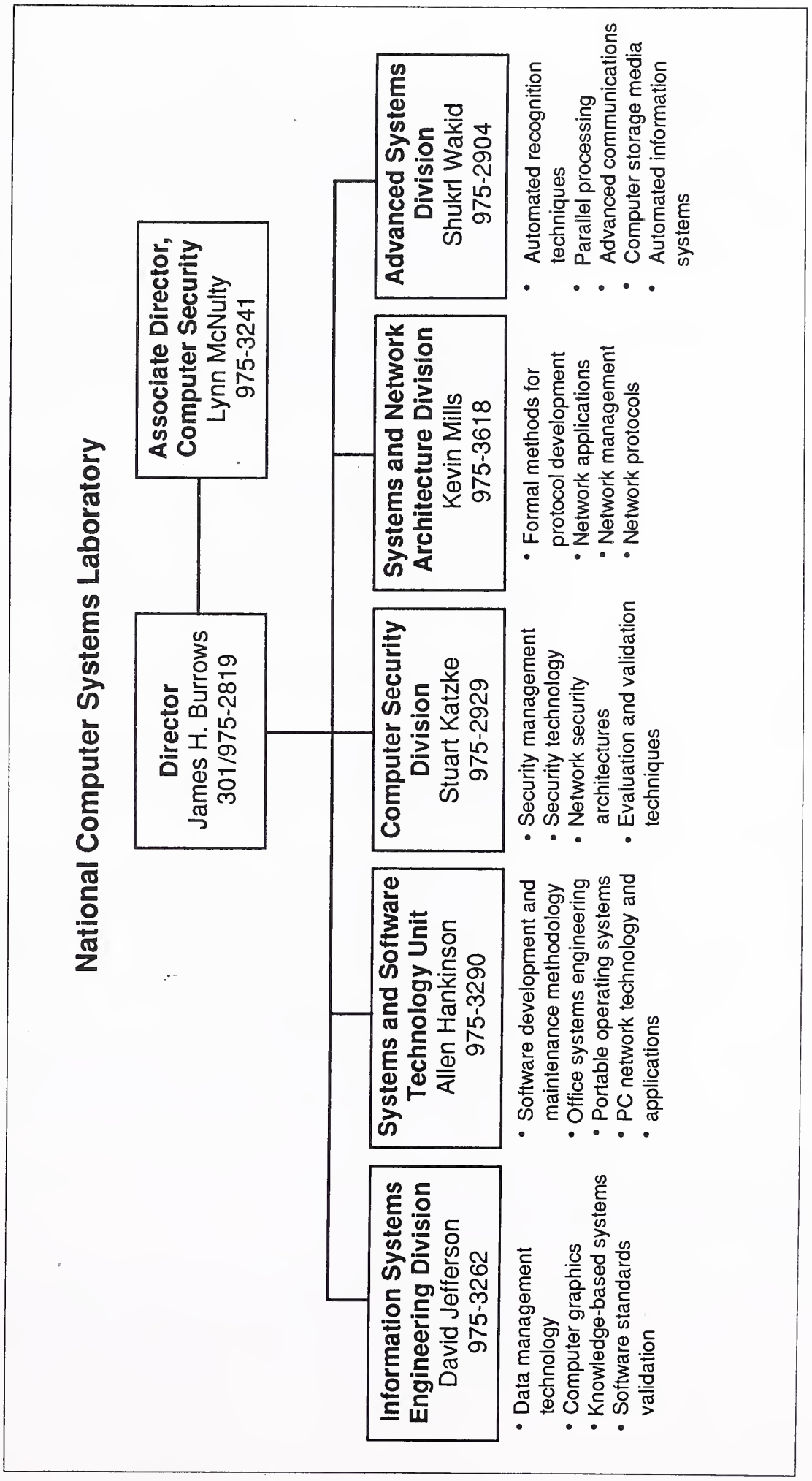
1. Identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer security and privacy

2. Advise NIST and the Secretary of Commerce on security and privacy issues pertaining to federal computer systems

3. Report findings to the Secretary of Commerce, the Director of OMB, the Director of NSA, and the appropriate committees of Congress

Membership on the Board includes both federal government officials and industry representatives who are eminent in the fields of computer and telecommunications technology.

EXHIBIT III-11



5. General Accounting Office (GAO)

The General Accounting Office has issued more than two dozen reports on federal computer security within the last five years. For example, in February 1989, GAO issued a highly critical report on federal compliance with the training requirements of the Computer Security Act. In another report, written before the Internet virus incident, GAO warned that most agencies, while expanding their computer systems, are not paying enough attention to security. In still another report, which accompanied congressional testimony given in July, 1989, GAO commented on the Internet virus, the factors facilitating it, the system vulnerabilities, and the factors hindering prosecution. One of GAO's most recent reports criticizes the Justice Department's management of ADP and computer security.

GAO's reports on computer security are not limited to criticisms. Some reports offer guidelines on managing security. One report, for example, offered suggestions for integrating computer security into other agency IRM functions. Another report made organizational suggestions to help agencies cope with the computer security threat. This included the establishment of a security "focal point" for interagency networks.

6. President's Council on Integrity and Efficiency (PCIE)

The PCIE, an interagency organization, did a survey of federal agencies' attention to computer security and compliance with the Act. The report criticizes agencies in the following areas:

- Technical Security Software Controls
  - Critical system files not adequately protected:
    - Sensitive utility programs not adequately controlled
    - Tape bypass label processing not adequately restricted
  - Special security exposure interfaces not installed

- Administrative Security Controls
  - Security not administered by independent staff:
    - Adequate policies, standards, and procedures not promulgated
    - Security violation reports not effectively reviewed

G
Federal Computer Security Vendors

In responding to federal computer security requirements, the vendor community has developed a variety of products and services, some operating in classified environments. No single vendor dominates the market, and perceptions differ among agencies and vendors.

Exhibit III-12 lists the vendors that agency respondents mentioned most frequently, as well as others mentioned. Exhibit III-13 lists similar response information from the vendors. Unlike the agency responses, which showed little in the way of priority, the vendor responses showed a definite pattern. It should be noted that, though Digital ranked first among vendor responses, it was not even mentioned by agency respondents. This suggests that Digital needs to improve its security image with federal agencies.

The remainder of this section highlights some of the products that vendors provide to meet federal computer security needs.

EXHIBIT III-12

Agency Views—Leading Vendors in the Federal Computer Security Market

- Vendors mentioned most frequently
  - Comsis
  - HFSI
  - IBM
- Other vendors mentioned
  - AT&T
  - CDSI
  - Computer Associates
  - EDI Audit
  - Fischer International
  - Grumman Data Systems
  - Mainframe Incorporated
  - Martin Marietta
  - SDS
  - TRW

Note: 35% of agency respondents were unfamiliar with specific companies or nonresponsive to question.

EXHIBIT III-13

Vendor Views
Leading Federal Security Vendors

Vendors	Rank*
Digital Equipment Corporation	1
AT&T	2
IBM	3
HFSI	4
Motorola	5
TRW	5
Xerox	6
Computer Associates	6
Unisys	6
Boeing Computer Services	7
Sun Microsystems Inc.	7
Trusted Information Systems	7

*Rank based on frequency of mentions by industry respondents.

1. Hardware Vendors

Most of the hardware market concerns Tempest-certified computers. Tempest certification relates to the features on some machines that are designed to limit low-level radiation emissions that are susceptible to eavesdroppers. Exhibit III-14 lists some of the leading Tempest vendors. For the most part, the list does not contain household names. Rather, it contains mostly companies that specialize in this market.

EXHIBIT III-14

Tempest-Certified Computers

Vendor	Equipment Market
Atlantic Research	Macintosh
CPT Corporation	Multiuser UNIX (Motorola Chip)
	AT-compatible (Intel Chip)
CR International	AT-compatible
Data General	Eclipse
Datasec	AT-compatible
	Macintosh
Datawatch	Multiuser UNIX (Intel Chip)
Delta Data	AT-compatible
Digital Equipment	PS/2-compatible
Grid	VAX
Hetra	Intel Chips
Hewlett-Packard	AT-compatible
International Technology	Vectra
	AT-compatible
Mesa Technology	PS/2-compatible
Mitek Systems	AT-compatible
Tempest Technologies	Macintosh
Wang	AT-compatible
Zenith/Inteq	AT-compatible
	VS minicomputer
	AT-compatible
	OS/2-compatible

In addition to its secure Macintosh, Mitek has developed a Tempest version of Cygnet's optical mass storage products. The product is referred to as an optical jukebox. Some other computer security products include:

- Minatronics provides a fiber optic cable device for physical protection of microcomputers.

- Eye Dentify provides retinal scanning devices for use in access control systems.

- American Computer Security Products provides a product called Immune System, which it refers to as a "virus-proof" 286-based microcomputer.

2. Software Vendors

Far more software vendors participate in the federal computer security market than do hardware vendors. This reflects both the perception of more software opportunities as well as the (usually) lower capital investment required. The majority of software products fall into two categories:

- Products that aim at specific NSA security levels, as defined in the Orange Book

- Products aimed at controlling access and protecting computer systems from viruses

Some of the products having current or pending NCSC certification are listed in Exhibit III-15. Because of the cost of time required for NCSC certification, some vendors are asserting "Orange Book" compliance without certification. Although this will not help in the federal market, it may be useful in some commercial activities.

The version of a software product is critical to its security reliability. For example, though VAX/VMS was certified for the 4.3 version, the 4.4 version contained a flaw that permitted access to NASA's Space Physics Analysis Network. The technical complexity associated with security verifications has led to some confusion among agencies and vendors. INPUT does not expect clarification any time soon, as some agencies look for ways to short-circuit the system.

EXHIBIT III-15

NCSC-Certified Products

Vendor	Product Names
AT&T	UNIX System V/MLS
IBM	VM/SP - RACF
Digital	VAX/VMS Version 4.3
Gould	UTX 32
Sun	SUN OS/MLS
Harris	CS/SX
Unisys	OS 1100
Trusted Information Systems	Trusted Xenix (formerly IBM's Secure Xenix)
Sybase	Secure SQL Server
Microsoft	OS/2
Informix Software	OnLine/Secure 4.1

The second major category of security software products relates to virus and access protection. Exhibit III-16 lists some of the key products in this area. The wide variety of (relatively) unknown products suggests that some industry shakeout is likely, particularly for products protecting microcomputers.

EXHIBIT III-16

Access/Virus Protection Security Products

Vendor	Product Name	Operating Environment
American Computer	Compusec II	Intel MS-DOS
	Immune	Intel MS-DOS
Bourbaki	Muscle	Intel MS-DOS
CH Systems	Sleuth	
Commcrypt	Cryptolock	Intel MS-DOS
Computer Associates	CA-Unipack/SCA	MVS
CXR Telecom	AJ Series	
Cylink	CIDEC-LS/HS	
	Secure PC	Intel MS-DOS
Dial-Guard	Dial-Guard	VAX, Tandem,
Digital Pathways	Defender II, SLS	MVS
Enigma Logic	PC-Safe II	
	VAX-Safe	Intel MS-DOS
	UNIX-Safe	VAX VMS
	Stratus-Safe	UNIX
	Tandem-Safe	VOS
	Virus-Safe	VOS
First Aid Software	Anti-Virus Kit	Intel MS-DOS
Fischer International	Watchdog	Macintosh
Foundation Ware	Certus	Intel MS-DOS
Harcom Security	PC-Watchman	Intel
HJC Software	Virex	Intel MS-DOS
International Security Technology	Virus-Pro	Macintosh
Jones Futurex	ENC-3XX	Intel MS-DOS
Kent Marsh	Nightwatch	Intel MS-DOS
Kinetic Software	Access	Macintosh
Lattice	Secret Disk	Intel MS-DOS
LeeMah Datacom Sec.	Traqnet 2000	Intel MS-DOS
	Infokey	
Paul Mace Software	Mace Vaccine	
Panda Systems	Dr. Panda Utilities	Intel
PE Systems	Guardsman 100	Intel
	Gillaroo	
Pyramid Development	PC/DACS	Intel MS-DOS
Racal/Guardata	PCSM	Intel MS-DOS
Racal/Vadic	VA930, 4492	Intel MS-DOS
Rainbow Technologies	Data Sentry II	Intel
RG Software Systems	Disk Watcher	Intel
	Vi-Spy	Intel MS-DOS
RSA Data Security	MailSafe	Intel MS-DOS
	RSA Sign/Check	Intel MS-DOS
Software Concepts Design	Flu Shot	Intel
Software Directions	Soft Safe	Intel
Technical Communications	Cipher X, CSD 3324A	
	DSD 72A SP, CSD 909	
	Raven, The Key	
Triton Products	Virus Guard	Intel
Telco Systems	Accelerator	
Worldwide Software	Vaccine	Intel

3. Network Security Vendors

Network security has received more media attention, although not necessarily more federal funding, as a result of the Internet virus and other viruses. However, it is widely believed that local-area networks (LANs) pose greater security problems. As might be expected, a wide range of vendors are offering network security products to federal customers:

- *LAN Investigator Plus* by Absolute Security Inc. provides customized scheduling of file verification, file modification detection, and some code management.
- *FoxMed* by ACC is an eleven-module integrated practice management system.
- *cCipher* by Access Technology Corp. is an encrypting and duplication system for software developers and network administrators.
- *TIP/30* by Allison-Ross Corp. provides multitasked program control, integrated message control, file control and security.
- *DES-Mate* by Arkansas Systems, Inc. provides data encryption for messages or data elements sent and received from IBM hosts participant in a network.
- *Telegate* by ASoftCo provides security/protection for prevention of fraud on PBX, Centrex, electronic key, voice mail and fax systems.
- *Auto Sig 3* by Autosig Systems, Inc. is a signature verification package.
- *VANguard* by Banyan Systems, Inc. offers audit trails and reporting tools, password encryption, and protection from unauthorized log-in or access to network traffic.
- *Net/Assure* by Centel Federal Systems provides network security for prevention of unauthorized use or access to a user's system, data, or network.
- *Central Point Anti-Virus* by Central Point Software, Inc. is a virus detection, removal, and prevention package.

IV

Federal User Requirements and Trends

This section describes the results of INPUT's past survey of federal agencies, as well as other agency information reflecting requirements and trends in computer security.

In general, agency responses showed a wide mix of opinions on present and future needs for computer security. Although everyone agreed on the need for network security, a plurality of respondents showed no established criteria for evaluating security products. This suggests some flexibility for vendors in responding to federal security needs. The market is not yet clearly defined.

However, a majority of agency respondents did not view past and current vendor efforts as successful. This suggests that at least some vendors need to change something in order to gain agency confidence. In particular, agencies mentioned delivery and support experience as areas where vendor improvement is needed. Vendors will also need to market heavily in order to overcome agency budget constraints and enhance market penetration.

A

Federal Agency Compliance with the Computer Security Act

During the past survey of federal agencies, INPUT asked what security measures the agencies had adopted to date pursuant to the Computer Security Act of 1987. Exhibit IV-1 identifies the measures already completed. The largest percent (86%) noted that their agencies had identified their sensitive systems. The percent reporting that systems were identified, 86%, probably reflects the entire government fairly accurately. As GAO has reported, most agencies made a legitimate effort to identify their systems. However, INPUT's sample probably reported a higher ratio of plans implemented (41%) to plans completed (68%). The GAO looked at security controls in 22 plans, and found that only 38% of those planned had been implemented. This suggests business opportunities for vendors who can help agencies implement the plans.

Under the Computer Security Act, sensitive systems were to be identified by July 8, 1988. Agencies could then proceed to establish a security plan for each federal system that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, unauthorized access or modification of the information contained in the system. Furthermore, according to the Act, a summary of the plan should be included in the agency's five-year plan.

As noted in Exhibit IV-1, sixty-eight percent of the agency respondents reported that they had completed the required security plans due to NIST by January 9, 1989. NIST reported receiving 1,000 plans, or approximately half of those required, by the deadline. OMB is responsible for ensuring that agencies have appropriate security plans in place; NIST and NSA handle review and evaluation of the plans. The plans ranged from one page to over 200 pages and addressed a variety of policy and procedural issues. The preliminary reviews by NIST and NSA indicated some shortcomings in awareness and training which will need to be taken up in future year submissions, if new plans are submitted.

At the time of INPUT's survey, 41% of the agency respondents indicated implementation of the security plans. Many agencies have begun training their employees in computer security awareness, while other federal agencies are still establishing security policies. The implementation phase varies among agencies due to the differing nature of security and number of sensitive computer systems at each site.

EXHIBIT IV-1

Computer Security Measures Adopted

Security Measure	Percent of Respondents*
Sensitive Systems Identified	86
Security Plans Completed	68
Security Plans Implemented	41

*Adds to more than 100% due to multiple responses.

The General Accounting Office (GAO) studied the compliance of the federal agencies in reporting the number of installed sensitive systems. Seventy-two agencies responded to the GAO inquiry. The total number of sensitive systems identified by the agencies reached 53,443 as of September 8, 1988. Exhibit IV-2 displays the number of systems for selected

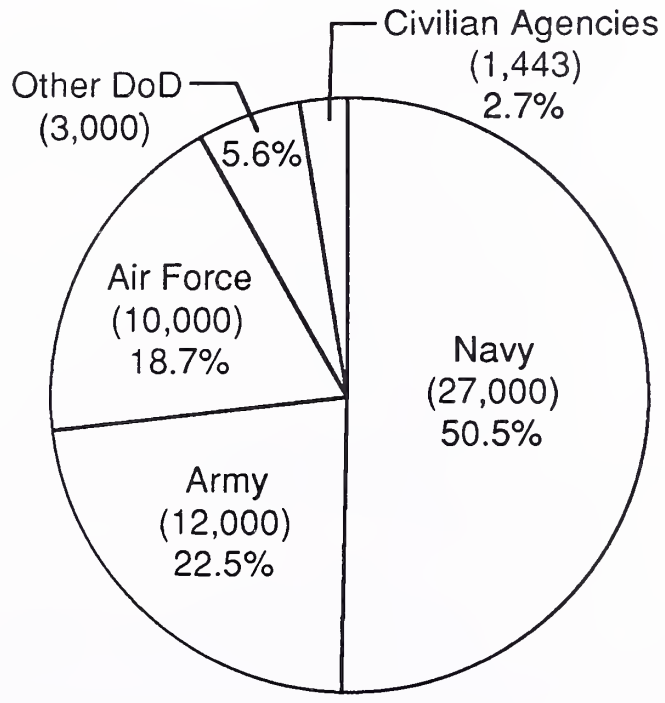
agencies and the proportion each represented of the total reported. The defense agencies reported an estimated 52,000 sensitive systems or about 97% of the total reported by all government agencies. The Navy, with 27,000 systems, is the single largest agency for sensitive systems.

Further research shows that many civilian agencies aggregated their systems, thus reducing the total number. Defense agencies, however, did not consolidate, which drove up their numbers. This suggests that vendors may pursue far more than the 53,000 systems that GAO identified.

According to NIST, the number of sensitive systems an agency possesses is directly proportional to the size of the agency. NIST identifies the Department of Health and Human Services as owning the second largest number of sensitive systems. NIST is trying to promote the philosophy that all computer systems are sensitive and not just those subject to DoD Orange Book classifications.

EXHIBIT IV-2

Number of Sensitive Systems Reported by Agencies as of September, 1988



Total Reported by 72 Federal Agencies = 53,443 Sensitive Systems

Source: Computer Security, Status of Compliance with the Computer Security Act of 1987, Briefing Report to Congressional Requestors, GAO, September, 1988.

Exhibit IV-3 illustrates the respondent views of the responsibilities of government agency staff for implementation of security measures. Nearly half (47%) of the staff was directly responsible for agency efforts for the design/implementation of policies. Under the Computer Security Act, each agency may employ computer security standards which at a minimum contain the standards made compulsory by NIST. Thirty-five percent of the respondents had total responsibility for computer security at their agency. It is viewed as advantageous for some agencies to centralize computer security responsibility in one office. Additional responsibility areas for agency personnel include oversight of adherence to standards and general management.

EXHIBIT IV-3

Agency Staff Responsibilities for Security Implementation

	Percent of Respondents
Design and/or Implement Security Policies/Guidelines	47
Total Responsibility	35
Ensure Adherence to Standards and Directives	12
Security Manager for Staff	6

In February, 1989, GAO published a report entitled, "Compliance with Training Requirements of the Computer Security Act of 1987." The GAO surveyed 85 agencies in connection with training progress, and found the following:

- Forty-five agencies have initiated computer security training.
- Nineteen agencies plan to start a training program.
- Two agencies could not say when they would start training.
- Fifteen agencies claimed that they have no sensitive systems.
- Four agencies did not respond to the survey.

GAO has not published a report on computer security training compliance since this 1989 report. It is unclear whether the GAO report compelled agencies to increase computer security training.

B

Future Computer Security Measures

In the future, more rigorous security programs and training will be needed by federal agencies to protect the integrity and privacy of information systems. Agency program managers are slowly gaining experience in establishing security requirements and developing plans. This should move the federal agencies closer to compliance to all provisions of the Computer Security Act.

Exhibit IV-4 reflects agency responses to questions about computer security measures planned for the future. The largest number (37%) of the respondents plan to implement security features in their computer software. In order to meet the agencies' needs, industry is developing modifications to DBMS products to meet B2 requirements, and network-based software to handle multiple-level access.

In January 1992, three DBMS products were being tested by the National Computer Security Center for basic C2-level security, which will be required of all agencies by the fall of 1992. The producers of the three packages are Informix Software, Oracle and Sybase.

EXHIBIT IV-4

Future Computer Security Measures

Security Measure	Percent of Respondents*
Implement Security Features in Software	37
Increase Security Training/Awareness	32
Implement Other Security Measures	27
Develop Contingency Plan	18
Conduct Risk Analysis	14

*Adds to more than 100% due to multiple responses.

Increased computer training and awareness will be undertaken by nearly one-third of the respondents over the next few years. To assist the agencies in complying with training requirements, the Office of Personnel Management issued computer security awareness training material to agency managers. OPM will continue to work with NIST and an interagency advisory group to develop and distribute additional training aids.

The survey findings indicated a wide range of other planned security measures that accounted for 24% of the responses. These other measures include:

- Achieving C2-level functionality by 1992 for all systems and networks
- Enhancement of monitoring devices and access controls
- Hiring of security program managers
- Conducting security reviews
- Obtaining certification of system designs

At the time of the survey, the federal agencies were also attempting to develop their contingency plans and risk analyses. Contingency plans allow agencies to have in place established routines and procedures for activation in cases of security violations. Each plan describes the appropriate response to situations that jeopardize the safety of data or information processing and communications facilities.

Risk analysis is an evaluation of system assets and vulnerabilities to establish an expected annual loss or equivalent for certain events, based on costs and estimated probabilities of the occurrence, or a ranking of the categories of risk of those events. The risk analysis should detect some of the serious security problems associated with federal information systems, thus allowing for installation of proper safeguards at the agencies. Controlled access, user authentication rules, passwords, encryption, and physical security controls are all options that need to be evaluated. Many agencies believe they should expedite the necessary risk analyses in order to ensure the security of their current and future systems.

Another security measure being taken with more frequency involves the procurement process. Many solicitations now have clauses relating to Contractor-Induced Computer Viruses (CICVs). This puts the burden and risk on contractors to insure that all delivered products are virus-free. Many solicitations now contain clauses that:

- Notify contractors that they are responsible for CICVs and that liability will be addressed under both the FARs and the FIRMRs

- Require proposals to identify the approach(es) for preventing CICVs

- Provide inspection and acceptance test clauses and CICV-free warranties

C

Vulnerability of Federal Computer Systems

Federal agencies' information systems are vulnerable to the harmful effects of natural and human-made hazards, which can impact the accuracy, integrity, and continuity of computer operations. Even with installation of mechanisms and techniques that control access to stored information, the physical and operational aspects of information systems lead to their vulnerability.

In a published report, Congressman Wally Herger indicated the presence of system vulnerabilities at NSA, the SDI office, EPA and the House of Representatives. In each case, computer virus penetration demonstrated the weaknesses of agency computer systems. The report also highlighted the need to improve computer security at nuclear power plants and air traffic control centers.

Exhibit IV-5 shows the agency respondents' views on which computer systems are most vulnerable to security problems. Microcomputers were named twice as often as either mainframes or midsize systems. The federal government has nearly 500,000 microcomputers in its inventory; thus the magnitude of potential computer security problems is huge.

EXHIBIT IV-5

Systems Most Vulnerable to Security Problems

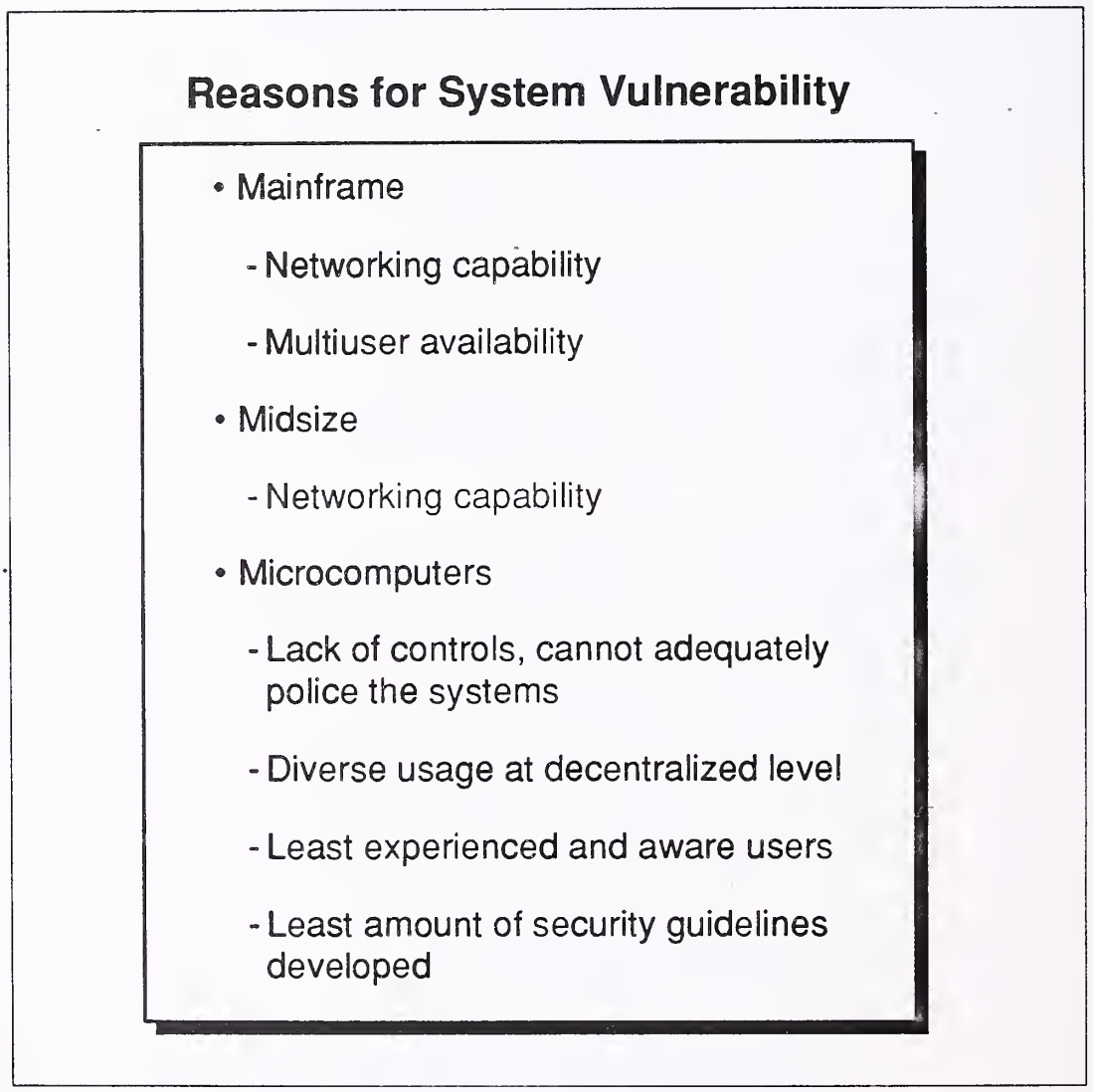
Type	Percent of Respondents*
Microcomputers	64
Mainframes	36
Midsize	36

*Adds to more than 100% due to multiple responses.

Executives in NIST's Computer Systems Lab also believe that microcomputers are more vulnerable to security problems than other types of computers, because the microprocessor platform by nature is less secure.

The networking capability of both mainframes and midsize systems is the most common reason for these systems' vulnerability, as is noted in Exhibit IV-6. Mainframes are also vulnerable because of multiuser availability. Greater system accessibility by a larger number of potential users substantially increases the risk for unauthorized manipulation of data and potential invasion of viruses. The respondents mentioned that security limits of gateways and network controllers leave systems vulnerable. Furthermore, the ability to access networks via telecommunications increases the risks of altered or destroyed data, or access by an unauthorized user.

EXHIBIT IV-6



The widespread use of microcomputers has exceeded the level needed for adequate control and policing of security policies for users. To compound the problems, usage is also decentralized. Geographically dispersed government sites with diverse functional/application areas contribute to the difficulties in regulating and developing standards and guidelines for

the security of microcomputer systems. In addition, respondents mentioned that micro users may not be as highly trained and aware of security measures. Less experienced users would not often detect irregularities or report unauthorized computer practices.

Officials at NIST believe that micros are vulnerable to security problems, because there is less capable security hardware and software available at the micro level than at higher computing levels. There are few security controls designed for a single user.

The agency respondents were asked to identify the major security threats to computer systems. The multiple responses are summarized in Exhibit IV-7. Seventy-four percent of the respondents indicated that data access was the main area of potential threat. This coincides with the agencies' heightened interest in password security and user authentication techniques.

The UNIX operating system, prominent in federal agencies, is very susceptible to security problems. UNIX is very conducive to an open software atmosphere and requires careful implementation of security measures. Without passwords and other security precautions, it is very easy for an unauthorized person to access critical files.

EXHIBIT IV-7

Perceived Computer System Threats

System Threat	Percent of Respondents*
Data Access	74
Data Manipulation	42
Software or System Manipulation	42
Site Access and Damage	21

*Adds to more than 100% due to multiple responses.

Data, software, or system manipulation were mentioned as perceived threats by 42% of the respondents. Manipulation by unauthorized sources can result in the loss of information, compromise of the accuracy/integrity of data and illegal access to sensitive information. Only 21% of the responses indicated that site access and damage was a serious threat. Apparently, physical entry of facilities and destruction of records or

equipment is not seen as much of a reality for some agencies, or precautions such as security guards, locked areas, and restrictive entry have already been implemented. Lack of access control, especially during non-working hours, was highlighted by GAO as a major security defect in the early 1980s.

The agencies were also mindful of the impact of increased end-user computing. Respondents noted an increased vulnerability to data manipulation and other security risks arising from the increase in end-user computing. Also mentioned was a need for increased awareness and security training for the users. Furthermore, agency respondents see a need to supplement the security regulations specifically for micros.

FTS 2000 does little to improve the security of end-user computing. It was not intended to be a secure network. However, both AT&T and U.S. Sprint are required to provide detailed call records as well as controls on access to the records. These controls are expected to meet C2 requirements, as defined in the Orange Book.

According to NIST, the volume of computer security problems is consistent across the agencies. Security problems seem to be directly proportional to the number of sensitive systems within an agency. Therefore, the Department of Defense bears the heaviest security burden. Other agencies publicly cited as having security problems include the Department of Justice, the Department of Commerce, and the Social Security Administration.

According to NIST, the key to managing computer security and problems that arise is through a structured security program. The following agencies possess effective and well-managed security programs:

- NASA
- DoD
- Energy
- State
- FAA
- Education

D

Protective Measures and Guidelines for Security

1. Agency Security Measures

Agencies need to rapidly move toward implementation of computer security measures in order to comply with already established and evolving security guidelines. The consequences of inadequate security controls in government systems are likely to become increasingly important in the

future. The federal government has been expanding its dependence on automated information systems to maintain and process a range of mission-critical, sensitive information. With increased government dependence on information systems and decentralized processing, government automated information systems will be subject to an increased range of vulnerabilities.

The Computer Security Act of 1987 requires the formulation of comprehensive security awareness and training programs for government agencies. Agencies must disseminate to their employees information on security requirements and safeguards that are critical to each agency's mission and operation of computer systems.

As shown in Exhibit IV-8, the survey findings indicated that less than half (45%) of the respondents were educating users and increasing security awareness as steps to protect their computers from viruses and other security violations. A substantial number of the respondents were not concerned with the use of properly authorized software, even though virus-infected software can quickly infiltrate a network. Only eighteen percent of the respondents specified intentions to implement an anti-virus software program. The cost of changing software over the life cycle of a system is an important hurdle that agencies must overcome in addressing technical software-related security issues, such as access control.

EXHIBIT IV-8

Measures Taken to Secure Computer Systems

	Percent of Respondents*
Educate Users/Increase Awareness	45
Use of Authorized Software Only	18
Issue Guidelines/Strategies	18
Implement Anti-virus Software	18
Other	18
Publish Alerts to Virus Outbreaks	9

*Total greater than 100% due to multiple responses.

The other security measures cited by the respondents included the following:

- Improve network monitoring
- Disallow bulletin boards
- Develop emergency response procedures
- Add layered security down to department level

The Bureau of Labor Statistics installed special software that generates secure digital signatures. The Bureau has 1,800 users on a 3COM Corporation network, connecting four Washington area sites with eight regional offices. From BLS' point of view, common software errors and natural disasters present a greater threat to data integrity than does malicious tampering. The digital signature approach also helps BLS to expedite its problem resolution activities.

GSA is addressing federal computer security by providing a data encryption service. It is close to implementing the service, which will allow federal agencies to send secured data files globally. The service is scheduled for release in October 1992.

The encryption service is being developed by GSA's Information Security Management Service and will permit agencies to send encrypted files either over FTS 2000 or International Federal Telecommunications Systems networks.

Another effort to facilitate computer security throughout civilian agencies was the organization of security teams within agencies to better battle computer attacks. NIST formed this loose network of Computer Emergency Response Teams (CERTs) several years ago. Unfortunately, most civilian agencies have not made efforts to form new CERTs, a recent NIST survey found. According to F. Lynn McNulty, associate director for security at NIST's National Computer Systems Lab, most agencies are not likely to establish CERTs until they themselves are attacked by viruses. This leaves the agencies unprepared to deal with an incident.

2. Training Programs

Section 5 of the Computer Security Act states that each federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each federal computer system. Such training shall be provided in accordance with regulations established by NIST and OPM prescribing the procedures and scope of training for federal civilian employees.

INPUT received diverse responses from the agencies on computer training initiated to date. Many respondents introduced general security awareness training, while others conducted more limited seminars and briefings on security issues. The majority of survey replies can be classified as either general instruction or targeted to specific personnel/user groups as follows:

General Instruction Training
- Internal seminars
- Annual security awareness bulletins
- Unit monitoring
- Classes conducted on a regular basis

Agency Personnel/ User Group Training
- New employees/ introductory level
- Supervisory staff (managers and officers)
- User training for security rules
- Employee training for accessing sensitive data

The majority of respondents did not believe that employee awareness of computer security required any additional training. However, the agency representatives did note an increased demand for end-user microcomputer controls and larger training requirements arising from the increased use of microcomputers. Updated training is also needed for newer computer technologies as well as more in-depth training in general.

Under Section 5(b) of the Computer Security Act, training must start within 60 days of the issuance of the OPM training regulation required in Section 5(c). OPM issued its interim training regulation on July 13, 1988; therefore the deadline was September 11, 1988.

In December, 1988 GAO requested information from agencies on the status of their compliance with sections 5(a) and 5(b) of the law. A total of 81 agencies responded to GAO and the findings are summarized below:

- Forty-five agencies reported starting their computer security training program as required by the Act.

- Nineteen agencies reported plans to start the training programs between November and April, 1989.

- Two agencies reported no set plans for the training program at that time.

- Fifteen agencies stated that they had no computer systems containing sensitive information.

The GAO report also reviewed the training tools used by the agencies. Thirty-one of the 45 agencies that had begun their training had a total of 190 different training courses and modules in use. Fifty-eight percent of the modules covered computer security basics, and 53% dealt with policies, procedures, and practices. Many of the 190 courses or modules were targeted to functional or program managers (56%), and at end users (50%). The training courses/modules also covered contingency planning and life cycle management.

In December 1991, OPM issued a final rule implementing the Computer Security Act of 1987, which requires training for all employees responsible for the management and use of federal computer systems that process sensitive information. Under the regulation, agencies will be responsible for identifying the employees to be trained and providing appropriate training. The rule lends the weight of OPM to gain overall compliance.

The announcement of the final OPM regulation was published in the Federal Register in December 1991. The Federal Register entry gave details of the rule, which will be a revision to 5 CFR part 930, subpart C.

3. Federal Agency Directives and Guidelines

Ninety-five percent of agency respondents report that they are adhering to their departmental computer security directives and regulations, as shown in Exhibit IV-9. The exhibit also indicates the breakout of DoD versus civilian regulations for the responses, with civilian agencies having a larger share.

Over half (55%) of the agencies identified other directives and guidelines. An extensive variety of security guidelines was cited. Those mentioned included the well-known publications such as the NSA's Orange Book as well as narrowly distributed defense agency security directives. OMB Circular A-130 was cited frequently because it contains the OMB security guidelines relevant to the development of automated information systems.

A surprising survey result included in Exhibit IV-9 is that only 9% of the responses acknowledged NIST's role in establishing security directives and guidelines. On the whole, the respondents' perceptions were that guidelines came from their departments, not a higher government-wide source, such as NIST or GSA.

EXHIBIT IV-9

Computer Security Directives and Guidelines

Policy Document	Percent of Respondents*
Departmental Directives/Regulations	95
- DoD 43%	
- Civilian 57%	
Other	55
OMB-130	23
NIST	9

*Total greater than 100% due to multiple responses.

The Computer Security Act itself specifies that NIST shall have the responsibility for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in federal computer systems. NIST shall draw upon the guidelines developed by NSA and also coordinate efforts with other government agencies including DoD, GAO, OMB, and the Office of Technology Assessment.

NIST has responsibility for federal unclassified computer systems and their security needs. NSA handles security issues involving classified information as mandated by the Warner Amendment. Currently, NIST and NSA are jointly developing government-wide security criteria to eventually be published as a FIPS document.

Some agencies are resisting NIST's oversight, further delaying the implementation of security procedures. It has been reported that many agencies are not identifying their sensitive systems, especially the LANs. A newly organized Federal ADP Users Group (FADPUG) Special Interest Group is aimed at helping agencies secure these systems, even if they have not been declared sensitive.

During INPUT's interview with NIST executives, eight possibilities for future legislation, regulations, rules or guidelines pertaining to federal computer security were discussed:

- Revision of the appendix to OMB circular A-130
- New specifications to replace the Orange Book
- Activity in the area of encryption
- Activity in the area of electronic commerce
- Revision of the Privacy Act
- Establishment of data privacy laws
- Citizen access to federal electronic records
- Proposed changes to the Computer Security Act

E

Functional Requirements and Performance Criteria

There is a broad spectrum of functional security requirements that can be applied to an information system. These range from relatively inexpensive and uncomplicated products (for example, use of passwords) to technically challenging and very expensive ones (i.e., A1 certification from the National Computer Security Center). Selection of functional requirements can significantly affect system costs, complexity, delivery schedules and performance.

Agency respondents gave multiple responses in identifying their particular agency's functional security requirements, which are compiled in Exhibit IV-10. All respondents specified network security. This requirement arises out of the agencies' operating environments, which are comprised of a growing number of PCs and workstations in LANs. Vendors are working to add security products that are either embedded in a computer's operating system or are add-on security packages suitable for the federal government's various networks. The major concern of agencies is their ability to maintain security across different networks.

End-user access includes user authentication, which identifies the user and verifies the user's eligibility for accessing the system. Functional safeguards to assure limited and proper access to sensitive data include encryption techniques, passwords, and multilevel security operating systems.

Functional requirements for data security were mentioned by 91% of the respondents. These requirements serve to protect the accuracy, integrity, and continuity of computer operations and processing of information for mission-critical and sensitive systems. Data security measures can utilize keys, passwords, log-on identifiers, and encryption techniques. Unresolved issues regarding data security include compliance with C2 requirements, porting to a security platform, and proprietary algorithms. Agencies will continue to add data security requirements to make their data tamper-resistant.

EXHIBIT IV-10

Functional Requirements for Computer Security

Requirement	Percent of Respondents*
Network Security	100
End-User Access	95
Data Security	91
Physical Security	86

*Total greater than 100% due to multiple responses.

Eighty-six percent of the agencies cited physical security requirements. These include limited or restrictive access to computer centers, remote processing sites, or LAN or WAN sites. Physical security is often the least costly and easiest functional requirement to fulfill. Employment of security guards, locked entrances, and limited accessibility are several available options for reducing system vulnerability. Some agencies, such as the State Department, are pursuing increased education and training as the best way to foster computer security. With so many foreign nationals employed at American embassies, it is especially important that all personnel recognize the need for computer security.

It is generally recognized that the most efficient and effective means to assure that a system contains the appropriate security controls and functions is to address computer security issues during the development of the system. Moreover, in cases where the security features of a system are an important consideration, it may be especially difficult to retrofit security into a system after it is operational. If the functional nature of the system is defined before security concerns are specified, system functional characteristics may be inconsistent with appropriate security objectives. In other situations, it may be technically or economically impossible to correct this problem. For example, certain security features, such as mandatory access control, may be difficult to retrofit into a system after the operational system and applications software have been accepted.

Agencies will find it easier to build in security in the initial development phases. However, the problem remains how to bring current information systems up to the level of security standards being mandated. For example, the IRS Tax System Modernization effort is forcing a rethinking of data security efforts. The agency is aiming for C2-level security in all its new mainline systems.

The federal agencies offered little comment on the performance criteria established for computer security products. Exhibit IV-11 indicates that 30% of the respondents had not established any criteria. One-fourth of the agencies interviewed were evaluating performance criteria in-house or at a departmental level. This method of evaluation tends to vary the expected performance among different agencies based upon their own information processing needs and types of systems, rather than promoting product uniformity.

EXHIBIT IV-11

Agency Performance Criteria for Security Products

Criteria	Percent of Respondents
No Established Criteria	30
In-house Evaluation/Criteria	25
Other Criteria	25
Control Access	20

The agencies' specification of controlled access to sensitive data and computer systems is indicative of their immediate demand for products that will protect information from outside manipulation and/or destruction. Products that establish appropriate procedures for access to networks, physical computer sites, and data bases each need to meet established agency performance criteria.

Additional performance criteria for security products mentioned by respondents include:

- Compliance with security architectures being drafted
- Low overhead costs

- Built-in software security
- Monitoring, auditing, and reporting capabilities
- Compliance with DoD C2 capabilities

Agency respondents evaluated the level of success for industry's satisfying the agency's current performance criteria. Exhibit IV-12 is based on agencies' experience with various vendors. The levels of success ranged from very successful to not successful, with two midranges of compliance with performance criteria.

EXHIBIT IV-12

Agency Evaluation of Industry Satisfying Criteria for Security Products

Degree of Success	Percent of Respondents
Very Successful	27
Moderately Successful with Future Improvements Needed	20
Limited Success	40
Not Successful	13

Some respondents (27%) viewed the computer vendors as already being very successful in providing products that comply with their agency's performance criteria. However, the majority (60%) of respondents categorized industry as having moderate or limited success to date. Some of the respondents—who indicated a current level of moderate success, with future improvements needed—suggested improvements providing greater protection of application software, easier implementation, and avoidance of retrofitting.

F

Acquisition Plans and Preferences

1. Acquisition Plans

As shown in Exhibit IV-13, eighty-two percent of the respondents indicated that their agencies would be adding software-driven password security over the next few years. A large portion of respondents also indicated that additional training tools and secure networking products would be acquired. These additional computer security acquisitions will support the agencies' compliance with required security standards and lessen the vulnerability of agency network systems.

EXHIBIT IV-13

Security Acquired through 1993

	Percent of Respondents
Software-Driven Password Security	82
Security Training Tools	77
Secure Networking Products.	68
Risk Management Analysis	59
Communications Security Products	55
Data Encryption Equipment	55
Other Contractor Support	50
Other Computer Security Devices	50
Contractor Assistance for Preparation of Plans	45
Secure UNIX-based Products	41
Secure Workstations	38
Tempest Products	27
Emission Control Devices	14

Over half of the respondents plan to acquire risk management analysis, communication security products and data encryption equipment. These services and products will further address the data security problems and end-user accessibility that are part of the major functional requirements for the security of information systems.

Although most of the agencies submitted their initial plans by the 1989 interview period, 45% of the respondents indicated planned use of contractor assistance for the preparation of computer security plans. Future computer plans may require some degree of contractor support, but not as much as in the earlier period of agency planning.

As noted in Exhibit IV-13, fewer respondents indicated intentions to acquire secure UNIX-based products, secure workstations, or Tempest products. These products in some cases are just beginning to find their role in civilian agency applications. Furthermore, additional product development and enhancements are still occurring, which may account for a wait-and-see attitude among agency respondents.

2. Method of Acquisition

Agency respondents were asked to comment on the planned method of purchasing computer security products. The respondents gave multiple replies to the acquisition methods they prefer to use, as shown in Exhibit IV-14. Multiple responses indicate that agencies expect to employ a variety of methods, depending on their particular needs.

EXHIBIT IV-14

Acquisition Methods—
Computer Security Products

Acquisition Method	Percent of Respondents*
GSA Schedules	85
RFP for Specific Purchase	60
RFP for Requirements Contract	55
Purchase Security Devices as Part of Other Procurements	40
Other Methods	20

*Total greater than 100% due to multiple responses.

Eighty-five percent of the respondents expect to buy from the GSA Schedule. GSA Schedule purchases will probably be used for agency purchases of software-related products and training tools, and additional items that are below approval thresholds. An almost equal share of respondents (60% and 55% respectively) indicated that their agency would use RFPs for a specific purchase or a requirements contract. There is a growing trend among federal agencies to use requirements contracts, and these may be extended into the computer security area.

Security products are also being acquired as part of other procurements. Respondents specified use of the Treasury TMAC and DMAC procurements as examples. Furthermore, respondents included in the other category generally use the open market and small business contracts.

The questionnaire also attempted to provide some indication of the trend approved in government agencies for acquiring the services of GSA-approved contractors to support their security needs. Thirty-two percent of the respondents stated that they already had or were planning to use a GSA contractor, and 45% of the respondents had no plans. The remaining 23% were undecided about the use of GSA contractor services.

Agencies that have already used contractors used them for risk analysis, planning, preparation of policies and guidance, and instruction implementation.

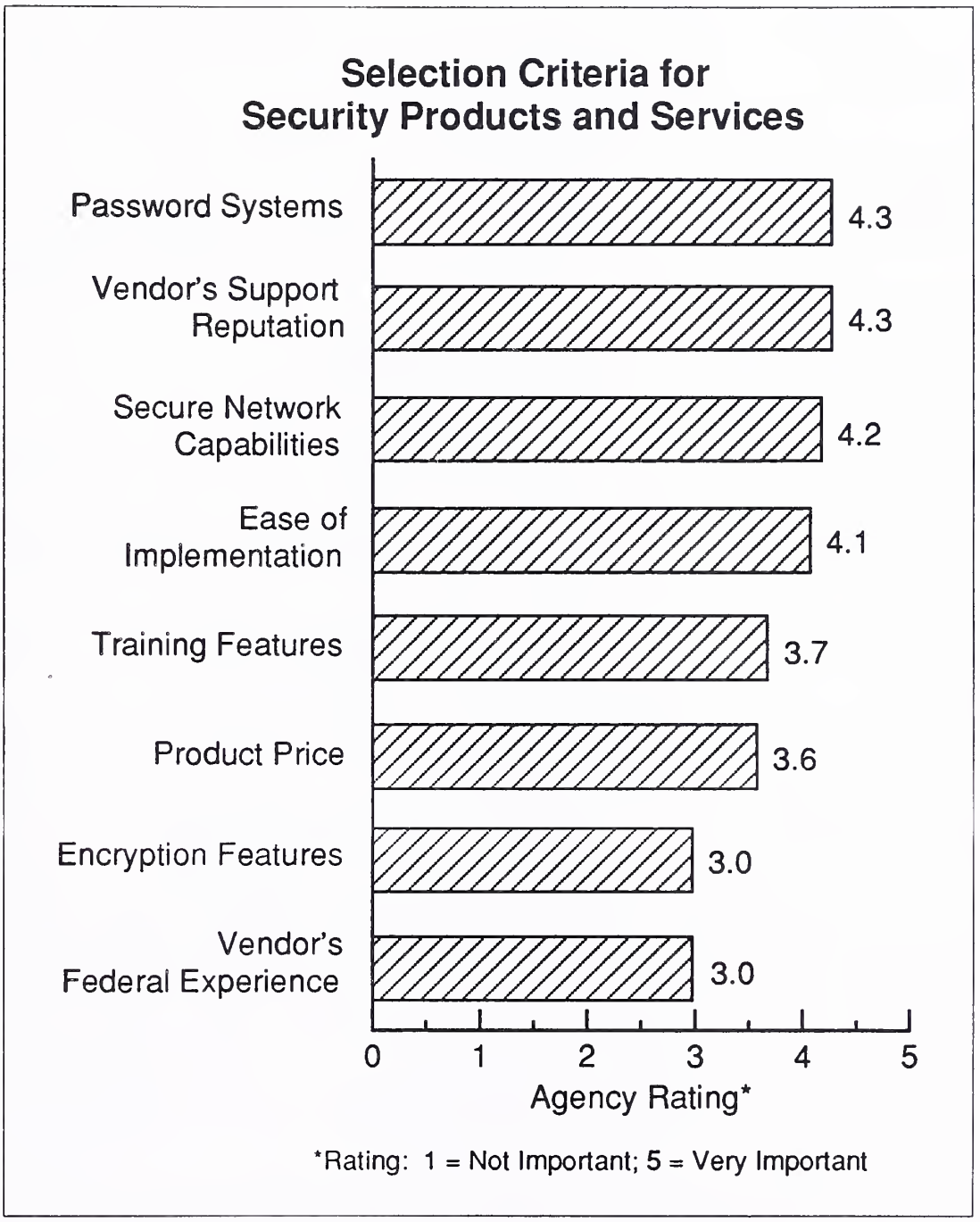
3. Product Selection Criteria

Agency ratings of the relative importance of various criteria in the selection of security products and services are shown in Exhibit IV-15. Password systems and vendors' support reputations tied for first place in importance. These two criteria reflect the current security emphasis at agencies, which need to install passwords that control access to systems. Agencies also focus on the reported support that vendors have been giving to their federal clients. A favorable reputation quickly spreads throughout the government, increasing the demand for products. A poor reputation is also passed on by word of mouth and is hard to overcome to capture additional federal sales.

The ratings for secure network capabilities and ease of implementation were also important factors for agencies and vendors. This again reflects the priority of agencies to resolve network vulnerability problems.

The extent of federal experience needed by the vendor was given the lowest rating by the agencies. Therefore, for selection of computer security products/services, the functionality and the positive support reputation of the vendor supersedes the vendor's government-related experience. In general, the ratings reflect a subtle shift in agency interest from performance to functional considerations.

EXHIBIT IV-15



G

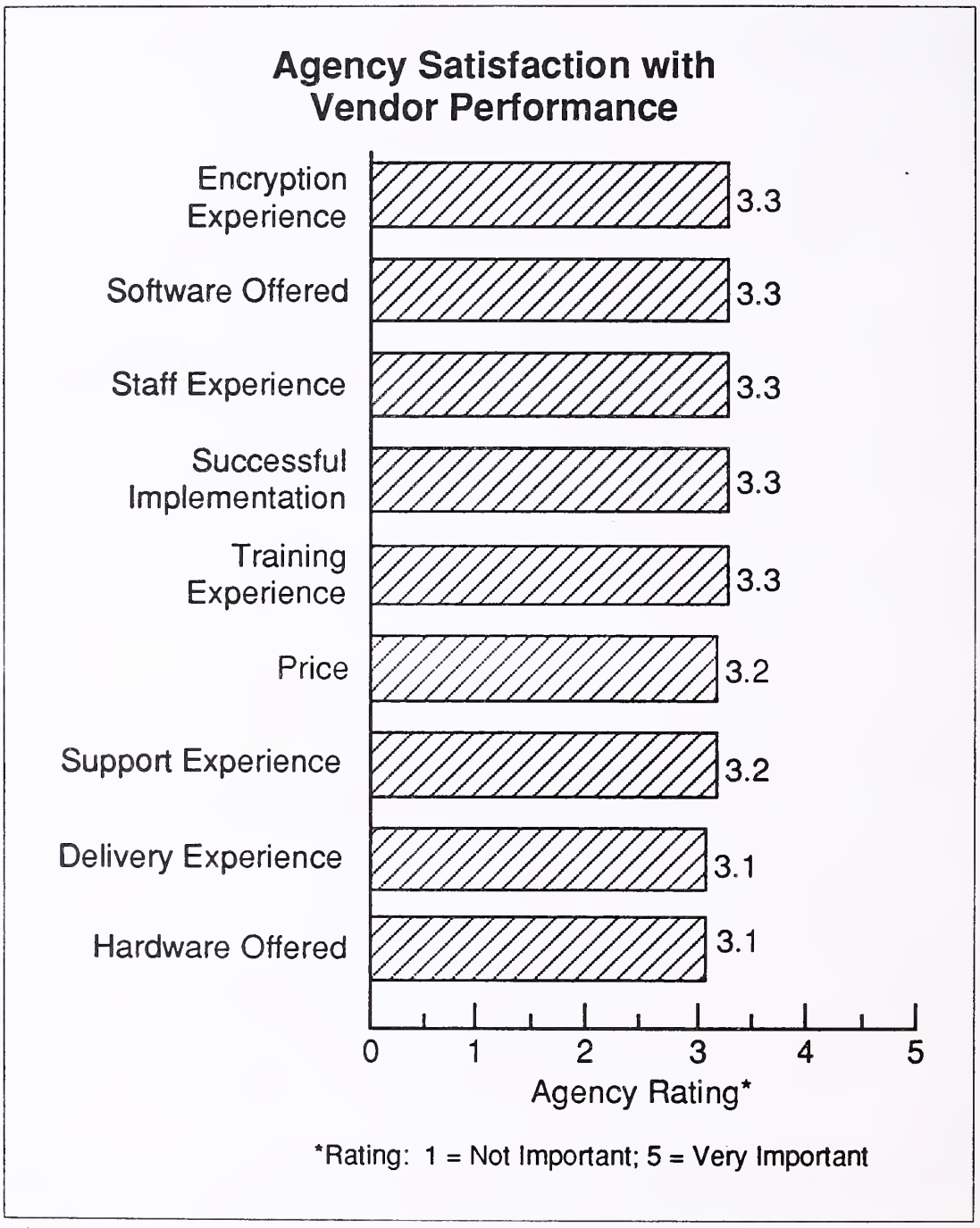
Vendor Performance

1. Agency Satisfaction with Vendor Performance

The overall level of satisfaction of agency respondents to vendor performance characteristics was moderate for all factors. Exhibit IV-16 displays the ratings given to each factor. Note that there are relatively few differences among the factors regarding vendor experience and product perfor-

mance; all received ratings in the 3.1 to 3.3 range. This moderate rating improved, however, as vendors became more familiar with agency security requirements that were unique to their missions or agency operations of sensitive systems.

EXHIBIT IV-16



2. Preference for Type of Vendor

Agency respondents were asked which type of vendor is preferable for providing appropriate computer security products and services for their agency, as shown in Exhibit IV-17. Sixty-five percent of the agencies preferred software vendors, and stated that these vendors are responsive to meeting a variety of agency security requirements with their products, and also provide product support as needed.

The next largest share (50%) of the respondents preferred hardware vendors and professional services firms because of their flexibility in providing the agency with various options and services. Most agencies do not view systems integrators as the most appropriate vendors for the installation of computer security products/services. However, as security requirements and features are installed on more networks and systems, the use of systems integrators may increase in the future. Systems integrators wishing to penetrate this area must augment their marketing efforts.

EXHIBIT IV-17

Agency Views on Appropriate Vendors for Computer Security Products/Services

Type of Vendors	Percent of Respondents*
Software Vendors	65
Hardware Vendors	50
Professional Services Firms	50
Systems Integrators	30
Aerospace Divisions	5
Not-for-Profit Firms	5

*Total exceeds 100% due to multiple responses.

3. Agency Suggestions for Improvements to Vendor Products and Services

Agency respondents were asked for suggestions on how vendors might make their computer security products and services more valuable to the federal government over the next five years. Exhibit IV-18 lists the principal suggestions made by the agencies. As should be expected, the replies varied due to the different types and levels of experiences the respondents have encountered with vendors. No ranking is available because of the diversity of replies from respondents.

The agencies are looking to future products to increase user education and security awareness. This is tied to the mandated requirements for employee training at federal agencies. The respondents also stressed the need for software-related security, at both applications and systems software levels.

Also mentioned were suggested improvements to the focus of the vendor's offerings to more of a government orientation. Apparently, respondents were expressing dissatisfaction with modified commercial offerings and want security products specifically geared to the government's mission and application areas. Furthermore, the products need to be available and delivered in a more timely manner.

EXHIBIT IV-18

Suggested Improvements to Security Products and Services

- Increase user education/awareness of security
- Integrate security into application and system software
- Increase government orientation
- Improve availability/delivery schedules
- Improve ease of implementation
- Stress security at development phase (avoid retrofit)
- Increase UNIX-based security products

As noted in other INPUT federal market studies, the agencies again suggested improvements to implementation. This shows that implementation of security products, along with other areas of software and hardware, still remains an issue with many respondents. Perhaps another suggestion made by respondents—to stress security at the system development phase—would eliminate some implementation problems. In addition, early incorporation of security features would avoid the costs and inefficiencies associated with retrofitting systems with security measures at a later stage. The solution lies both with the agencies in stating requirements and with the vendors in providing for these measures.

Although not cited by the majority of respondents, a small group of respondents suggested that vendors increase their UNIX-based products. As stated earlier, the UNIX operating environment is conducive to an open software atmosphere, which in turn could lead to security problems. There is an increasing demand for UNIX-based security products.

H
Trends

1. Technology Trends

Agency representatives were asked to identify technological factors that could affect their agency's future computer security requirements. Numerous factors were identified and those mentioned most frequently are listed in Exhibit IV-19.

EXHIBIT IV-19

Technological Trends Affecting Computer Security

Trend/Factor	Rank*
Expanded Networks/LANs	1
Intersystem Compatibility/OSI	2
Increased Use of Microcomputers	3
Advancements in Security Devices/ Safeguards	4
Developments in Telecommunications	5
Image Processing Technology	6

*Rank based on frequency of mention by respondents.

Many respondents identified expanded networks (especially local-area networks) and distributed processing network availability as important technological factors impacting their agencies' security requirements. The additional and more complex networks could increase access control problems and system vulnerability. OSI security is also causing some concern. Although the Government Open Systems Interconnection Profile

(GOSIP) has gone into effect, security problems have not been resolved. It is widely believed that OSI security has been delayed by a lack of standards. Since GOSIP emphasizes ease of access, it creates an opportunity for security violations.

Intersystem compatibility and implementation of OSI, though contributing to the flexibility and adaptability of governmental information systems, also amplify most of the existing computer security problems and possibly pose new ones. Agencies need to be able to achieve greater productivity via OSI over the next few years and still protect their sensitive data.

The respondents also mentioned increased use of microcomputers as a significant factor affecting future computer security requirements. As noted earlier, microcomputers already pose serious security problems that will be compounded with the increase in the number of users. It is difficult to enforce security regulations on users of microcomputers. Furthermore, these computers are geographically dispersed among different user groups and applications, and therefore more accessible and subject to unauthorized and possibly infected software.

On the positive side, the agencies did see future technologies bringing about advances in computer security devices to better serve the growing demand for products. Examples of enhancements to system safeguards included improved encryption techniques, software logging procedures, and secure optical disks.

Telecommunications developments such as fiber optics will impact the security requirements and products sought by agencies. The introduction of supplemental methods of communicating between systems or accessing a network will increase the security features needed for systems.

Image technology allows users to electronically store, process, and retrieve information, including text and graphics, on a computer. As this technology and related products become widely available, managing the security efficiently and still achieving productivity and savings gains will be a challenge for the 1990s.

Agency respondents also gave their views on the impact that the technological advances mentioned will have on computer security requirements and computer operations. Respondents clearly perceived greater difficulties in the future for controlling system accessibility and protecting data integrity arising from advanced technologies. They also expressed their concerns for ease of implementation. In addition, some agencies foresaw a favorable influence as the new technologies will increase the flexibility of system security and allow for more appropriate tools to be designed. Lastly, the respondents were hopeful that the increases in LANs and networks will eventually lead to development of specialized safeguards for networks.

NIST has taken a somewhat unusual approach in assessing the impact of technology trends. In 1988, NIST established the Risk Management Research Laboratory to advance leading-edge technology in assessing and managing computer-associated risks. Initially, the lab evaluated two dozen risk assessment packages. These packages were then used for constructing a conceptual framework for risk management. The lab will now assemble risk scenarios and evaluate the effectiveness of the framework.

During INPUT's recent interview with NIST executives, INPUT asked how technological changes are affecting agencies' computer security requirements. The executives stated that because of technological advances, information has become accessible to all via networks. The more technology advances, the harder it is to protect data and limit accessibility. Changing technology limits agencies' ability to focus controls and increases the spread of connectivity. Improvements in technology also create a paperless environment, which further increases the need for computer security.

2. Industry Trends

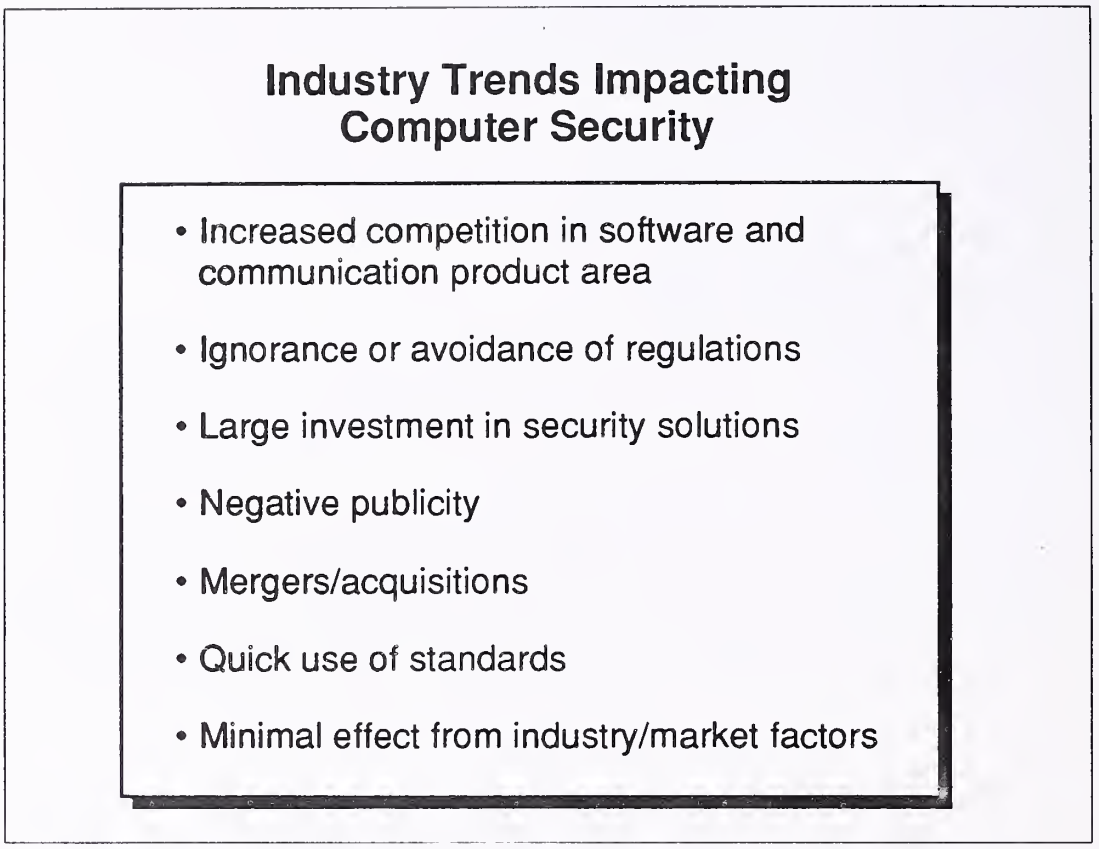
The agency respondents were asked to identify industry trends and non-technical factors that could significantly impact the agency's computer security plans. Exhibit IV-20 summarizes the agency responses. There is no ranking because of the diversity of the responses.

Many of the respondents mentioned increased competition for software and communications products. Several companies traditionally in the federal software and communications market have expanded into computer security products. Other sources of competition are commercial sector computer security firms, which are now targeting the federal market, along with start-up federally oriented security companies.

Mergers and acquisitions in the industry will continue during the 1990s. In some cases, depending on the product/service offered, a large investment of-capital may be required to develop and provide the security solutions geared to the government's mission and applications. Vendors with a strong financial background and good management skills will be best suited to survive the financial risks involved with the market.

The respondents expressed views on both sides of the compliance issue. Some indicated that vendors ignore or avoid regulations, while others noted quick adherence to standards. Since federal agencies are required to adhere to specific standards and regulations, companies that offer products that comply are expected to gain a stronger foothold at the agencies.

EXHIBIT IV-20



Publicity regarding computer viruses and other attacks on the security of government computer systems will also impact the federal computer security market. Agency respondents are concerned that too much notoriety will spur other acts of computer vandalism. Also, negative publicity tends to increase congressional and public inquiries into security operations, further complicating computer plans and requirements.

3. Budgetary Constraints

The majority of the agencies surveyed said that they experienced budgetary constraints attributable to the Gramm-Rudman-Hollings Act or other federal government budgetary constraints. Exhibit IV-21 shows the variety of impacts resulting from budgetary cuts on the development and implementation of computer security plans at the respondents' agencies.

The most frequently mentioned impact was that budgetary constraints have a "devastating" or highly significant effect. This implies that implementation has been seriously hindered or cancelled by lack of funding. Specifically targeted cuts have occurred in agency security awareness and training programs.

EXHIBIT IV-21

Impact of Budgetary Constraints

Impact	Rank*
"Devastating effect"	1
Cuts security awareness and training programs	2
Limited impact/restricts flexibility	3
Difficult to fund planned/additional programs	4
Limits staffing levels	5
Delays network encryption	6

*Rank based on frequency of mention by respondents.

Some agencies have suffered major delays and cutbacks in acquisitions, and other agencies have downsized levels of support and slowed their implementation efforts. Several agencies commented that at present they have encountered a minimal amount of budgetary constraint, but foresee more significant funding restrictions in the future.

According to NIST, budgetary constraints have a significant impact on agencies' ability and willingness to implement computer security plans. Agencies have difficulty budgeting for security needs. There is no category in agencies' mandatory budget submissions for computer security. They are supposed to include these costs in the overall system management category. Agencies find it difficult to reallocate funds for computer security. Also, computer security has to fight for new resources during the budgeting process. Traditional programs seem to receive continual funding while computer security must fight with new programs to receive funding. Finally, there is no national security requirement for non-DoD systems, which makes agencies less willing to spend funds on security they may view as nonessential.

4. Impact of Government Policy Agencies

Computer security for federal information systems is subject to a range of governmental policies, regulations, and other influences from policy-formulating agencies. Therefore, the agency respondents were surveyed to obtain their views on how several government regulations and policies

from selected agencies would impact their agency's computer security requirements and acquisitions in the future. Exhibit IV-22 shows each agency studied, and the general responses of agency officials. (A previous discussion of security regulations and policies was included in Chapter III.)

EXHIBIT IV-22

Respondent Views on Impact of Government Policies

- NIST
  - Set standards/guidelines to follow
  - Compliance may require increased training and security reviews
  - Manage relevant FIPS
  - NIST efforts benefit agencies
- NSA
  - Provide helpful assistance
  - Greatly impact COMSEC environment
  - Provide review and certification for products
  - Publish guidelines for encryption
  - Directly impact classified data systems
- GSA
  - Minimal/little impact
  - Improve contract methods
  - Publish security regulations
  - Uncertain of impact of FTS 2000

In general, respondents viewed the activities and security guidelines provided by NIST and NSA as beneficial. In complying with the standards and guidelines set, some respondents noted the possibility of having to increase their training and security reviews. The majority of respondents view GSA as having minimal impact on the federal computer security market.

NSA's area of impact is more apparent in the product evaluation/certification process and the COMSEC environment. NSA product approval is avidly sought by many vendors. The agency also has a strong role in establishing security procedures for classified data systems.

Respondents also commented that they expect GAO and agency Inspector General internal audits to increase reviews and oversight in the security area. In addition, it is expected that OFPP will be more active in establishing overall government strategies. Agency officials further anticipate that future legislation will required additional procedures to be implemented. This may result in the need for additional consulting services and installation of new tools.

The NSA headed two programs to foster the development of secure communications equipment for both classified and unclassified applications. The programs were referred to as Project Overtake and the Commercial COMSEC Endorsement Program (CCEP).

Project Overtake's mission was to develop a family of seven cryptographic modules for use by integrators and telecommunications equipment manufacturers. Companies that participated in Project Overtake included:

- AT&T
- GTE
- Harris
- HFSI (formerly Honeywell)
- Hughes
- IBM
- Intel
- Motorola
- RCA
- Rockwell

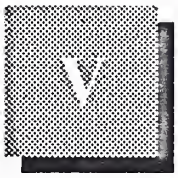
CCEP was established by NSA to ease the access of defense contractors and other organizations to encryption equipment. NSA provides the encryption devices and algorithms for these products, while the manufacturers package the products and build the user interfaces.

NIST is also having an impact in still another way. It has established a government-wide information network on security issues called the Forum of Incident Response and Security Teams (FIRST). FIRST was set up to do the following:

- Supply the latest information on security threats
- Develop a program to report and assess security incidents
- Offer assistance

Several agencies are working with NIST on FIRST, including Energy, Justice, Transportation, NASA, and the National Science Foundation.

FIRST is supposed to provide a formal link among agency Computer Emergency Response Teams (CERTs), which were also initiated by NIST. Unfortunately, most agencies have not established CERTs and approach security problems in a retroactive manner.



Competitive Trends

This section presents the results of past vendor surveys and other competitive information.

Vendors who responded to this survey provide a wide range of products and services to the federal computer security market. They also generate different levels of revenue. However, very few derive a large portion of their revenue from federal computer security. This suggests that security is an ancillary activity for most firms.

Although the vendors favored defense agencies for security sales opportunities, Treasury ranked first in terms of agency opportunities. This suggests that many vendors recognize the special security concerns at Treasury and intend to participate in Treasury business.

In general, vendors expect their computer security revenues to increase. They view the market as better defined than do agency respondents. However, they do show concern for the complexity of requirements and the relative lack of standards.

A
Vendor Participation

1. Vendor Products and Services

Exhibit V-1 shows the products and services that the vendors surveyed indicated they sold to federal agencies. Presently, the vendors' offerings emphasize secure network products, communications security, and software-driven password security. These are some of the same product areas that the agencies indicated earlier in Exhibit IV-13 that they would be acquiring in the future.

EXHIBIT V-1

Products and Services Provided to Federal Agencies

Products/Services	Percent of Respondents*
Secure Networking Products	64
Communications Security Products	57
Software-Driven Password Security	57
Data Encryption Equipment	54
Contractor Assistance for Preparation of Plans	50
Other Contractor Support	50
Secure UNIX-based Products	46
Secure Workstations	43
Risk Management Analysis	32
Other Computer Security Devices	32
Tempest Products	29
Emission Control Devices	21
Security Training Tools	21

*Total exceeds 100% due to multiple responses.

Some of the vendors interviewed are new entrants to the market and their responses covered planned products. The majority of industry respondents also noted that they plan to provide additional security products and services in the future in response to demands from government clients.

2. Vendor Respondent Revenue Characteristics

The vendor respondents represented many of the largest hardware and software suppliers to the industry as a whole and to the federal government sector. Also included are some of the specialized computer security firms. The majority of the vendors surveyed had revenues between $1 and $10 billion at the time of the survey.

The distribution of the surveyed companies' revenues derived from the federal computer security market is shown in Exhibit V-2. The largest share (41%) of respondents obtained approximately 1% of their revenues from this market. However, most vendors were optimistic about increasing this segment of their federal business. Federal computer security did not represent a majority of revenue for any of the vendors surveyed.

EXHIBIT V-2

Current Percent of Vendor Revenue Derived from Federal Security Market

Percent Revenue	Percent of Respondents*
0	12
1	41
2 to 5	6
5 to 10	18
10 to 20	12
20 to 80	0
80 to 90	6
90 to 100	6

*Total may not equal 100% due to rounding.

3. Industry Leaders in the Federal Computer Security Market

A ranking of the leading vendors in the federal computer security market, based on the frequency of mention by industry respondents, is provided in Exhibit V-3. For the most part, these companies have demonstrated the capabilities to comply with security standards and incorporate security processes and technology into their products and services. These help to satisfy the federal agencies' needs for end-user computer and networking security.

The companies mentioned most frequently—such as Digital, AT&T, and IBM—are moving into the security market through existing hardware product lines and supporting products in order to retain their foothold in the federal marketplace. Furthermore, many of the companies listed in Exhibit V-3 are also leading suppliers to defense agencies and thus gear their products to comply with the security standards essential to defense computer systems. Other companies mentioned are becoming well known for their workstation products, which are being modified to incorporate government-required security features.

It is interesting to note that the top five vendors in the list are principally associated with computer equipment. This suggests a perception on the part of the vendor community that computer security is focused on hardware.

EXHIBIT V-3

Leading Federal Security Vendors in Vendor Perspective

Vendors	Rank*
Digital Equipment Corporation	1
AT&T	2
IBM	3
HFSI	4
Motorola	5
TRW	5
Xerox	6
Computer Associates	6
Unisys	6
Boeing Computer Services	7
Sun Microsystems Inc.	7
Trusted Information Systems	7

*Rank based on frequency of mention by industry respondents.

B

Vendor Market Perceptions

1. Federal Agency Opportunities

The majority of the industry respondents provide their products and services to both the DoD and civilian agencies. INPUT asked which agencies can be identified as the best opportunities for a given company in the computer security market. The major defense agencies and NSA, along with several large civilian agencies such as Treasury, Energy and Justice were mentioned most frequently, as shown in Exhibit V-4. Besides the civilian agencies listed, other agencies listed by the respondents include Transportation, HHS, Agriculture and Commerce.

EXHIBIT V-4

Leading Agency Opportunities for Security Products and Services

Federal Agency	Rank*
Treasury	1
Air Force	2
National Security Agency	3
Navy	4
Army	5
Defense Intelligence Agency	6
Defense Communications Agency	7
Central Intelligence Agency	8
Energy	9
Justice	10
NASA	11
Defense Logistics Agency	12

*Rank based on frequency of mention by industry respondents.

For many vendors, the defense agencies are long-term targets for their products and services, since they are already well known at these agencies. The civilian agencies are considered a growing market segment, in view of additional security requirements the agencies are adding to comply with government legislation. Additional technological advances and product availability will fuel both of these market segments.

2. Differences Between Defense and Civilian Agency Markets

Exhibit V-5 presents the industry respondents' opinions on the differences between the defense and civilian agency markets for computer security products and services. The majority of respondents noted that more numerous and stricter requirements and standards are imposed upon the defense agencies than on the civilian agencies.

EXHIBIT V-5

Agency Security Market Differences

Defense Market	Civilian Market	Rank*
More stringent requirements and standards	Fewer mandated requirements and standards	1
Greater security awareness and experience	Less awareness/greater need for training	2
Larger volume of classified data/greater concern for national security	Less classified data/concern for authentication and integrity of sensitive data	3
Closer adherence to software development standards and customized systems	More reliance on hardware only/reluctant to invest in software due to cost	4
Require military-grade encryption and higher levels of security	Can utilize DES-based encryption and lower level of security	5

*Rank based on frequency of mention by respondents.

The second most notable difference was the greater level of security awareness at defense agencies and a more experienced staff. At the civilian agencies there is a greater need for training to bring them up to the level of awareness required by the Computer Security Act. This training is already under way at many agencies.

The mission of the defense agencies results in a larger volume of classified data and higher imposed levels of security. The classified systems and the concern for national security also result in an increased potential at some defense agencies for customized security systems and software.

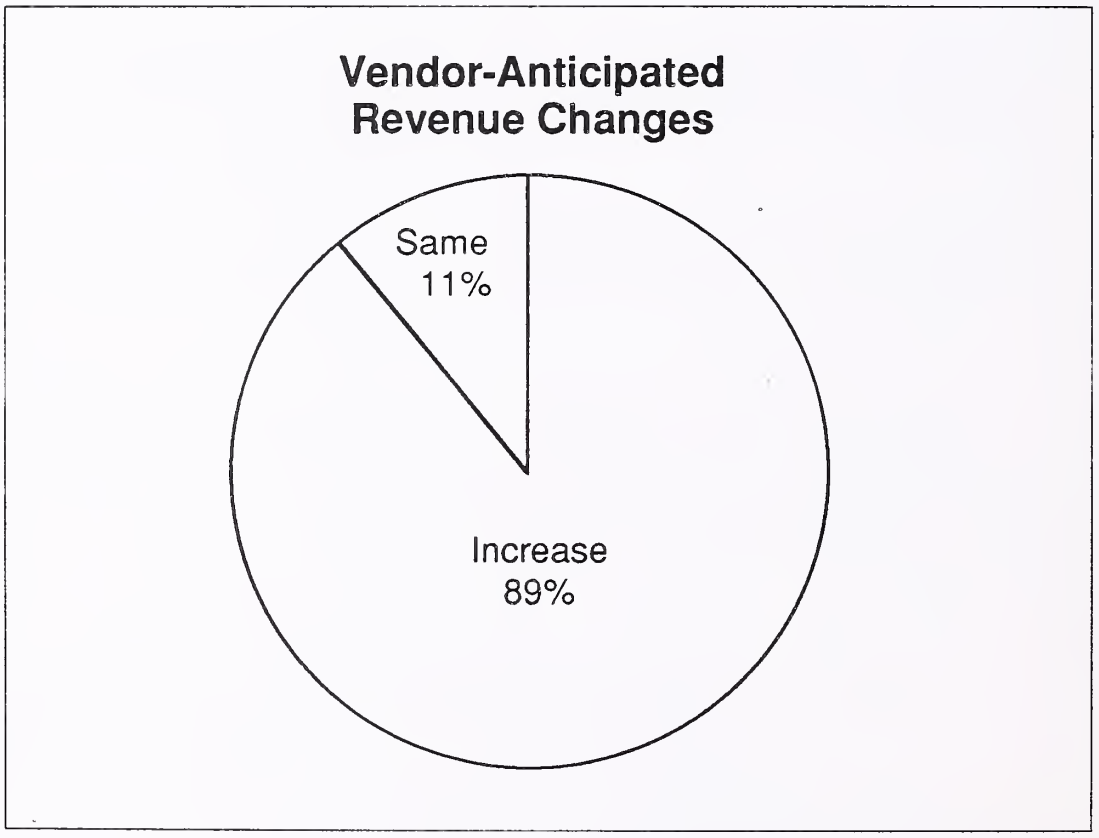
At the time of the survey, the civilian agencies were focusing on hardware-based security solutions and were not as willing to invest as much as the DoD to acquire software for computer security implementation. Because their volume of classified data is much lower, most civilian agencies

are able to utilize lower levels of security to protect the authenticity and integrity of their data. However, communications security is becoming very important in some civilian agency processes, such as those dealing with cash management and electronic funds transfer.

3. Anticipated Increases/Decreases in the Federal Computer Security Market

Most of the vendors surveyed expect their revenues from the federal computer security market to increase over the next five years, as illustrated in Exhibit V-6. None of the respondents forecasted a revenue decrease, and only eleven percent believed that revenues will remain at their present levels.

EXHIBIT V-6



Vendors also anticipate increases in their market share as a result of six main factors. Exhibit V-7 shows that many respondents (29%) expect their revenues to increase as the government increases its security requirements. Technological improvements and implementation of additional standards will also cause revenues to rise as the market expands and new products are made available. Several respondents are new to this market, and consequently have only a small market share. New vendors expect their revenues to increase as they participate in larger procurements.

EXHIBIT V-7

Reasons for Vendor Revenue Increase

Reason	Percent of Respondents*
Increased Security Requirements	29
New Products Available	25
Expanding Market	25
Increased Government Demand	18
New in Market	7
Increased Security Awareness	7

*Total greater than 100% due to multiple responses.

Vendors who believe that the federal computer security market will be leveling off indicated that budgetary cutbacks, the lengthy certification process, and market penetration would be the key forces holding down growth. Potential limits to funding and a more competitive arena could pose strong threats to the well-known vendors in this market.

INPUT forecasts that the federal computer security market will grow at a compound annual growth rate of 5% through 1997. Exhibit V-8 presents the market growth rates estimated by the industry respondents. The largest number of responses were in the 10% to 15% and 20% to 25% growth ranges. Overall, there was a high level of optimism among some respondents, with 15% of those surveyed estimating growth of 50% or more for the forecast period. The future of the federal sector of this marketplace is viewed more positively than the future of the security industry in general.

EXHIBIT V-8

Estimated Market Growth in the Next Five Years

Percent Estimated Growth	Percent of Respondents
Under 10	11
10 to 15	26
15 to 20	7
20 to 25	22
25 to 30	7
30 to 50	11
50 and up	15

*Total may not equal 100% due to rounding.

4. Advantages to the Federal Computer Security Market

Vendors surveyed by INPUT had wide-ranging opinions on the advantages of competing in the federal computer security market. Their responses are summarized in Exhibit V-9.

The industry respondents noted their ability to build on their previous computer security experience and recognition in the industry. This enables them to penetrate the federal market more quickly than some other market segments. Their early successes also reveal more opportunities within the government. They believe that the federal security market has the benefit of already having established requirements and standards with which the vendors must comply, rather than being in the midst of evolving standards.

Computer security at federal agencies entails some large-scale procurements with sizeable dollar values that attract vendors to the federal marketplace. Parts of the civilian sector could become a volume-oriented market, creating multiple opportunities due to the similarity of hardware

and software solutions that can be used in a variety of applications. Vendors also noted that the federal market is a precursor to the commercial market, and early developmental efforts are financially rewarded with the future demand for commercial off-the-shelf products.

EXHIBIT V-9

Advantages in the Federal Computer Security Market

Advantage	Rank*
Leveraging Experience and Industry Reputation	1
Well-defined Requirements in Most Areas	2
Meaningful Standards already Established and Being Adopted	3
Size of Contracts (large)	4
Development and Demand for Commercial Off-the-Shelf Products	5

*Rank based on frequency of mention by industry respondents.

5. Problems in the Federal Computer Security Market

Vendor views of the problems or disadvantages associated with this segment of the federal marketplace also span a wide range, as shown in Exhibit V-10. The most frequently mentioned problem is the necessity of complying with complex requirements and standards. Vendors expressed their frustration in trying to supply products that are compliant with highly technical and rigid standards.

Federal budgetary constraints pose a problem to vendors as agencies are not allocating significant funding for the implementation of computer security. The agencies are mindful of the need to avoid expensive retrofitting of systems, but have not yet made a full-fledged effort to build in security as systems are developing.

EXHIBIT V-10

Problems Associated with the Federal Computer Security Market

Problem	Rank*
Complexity of Requirements/Standards	1
Lack of Funding/Low Budgets	2
Lack of Awareness/Educated Users	3
Lengthy Product Certification Process	4
Lengthy Procurement Process/Threats of Protests	5

*Rank based on frequency of mention by industry respondents.

Presently, industry respondents are facing the problem of dealing with users who are lacking in security awareness and training. This hampers the demand for security products as well as making implementation more difficult. The required level of sensitivity does not yet exist in many agencies. Although some marketing will help, budget constraints will continue to dampen market growth.

Vendors are burdened by both a tedious and lengthy product certification process and the federal procurement process. These long procedures prevent companies from bringing products to the market in a timely manner. They can also cut into the potential for company profits.

Other concerns mentioned by vendors were:

- User acceptance/compliance
- Obtaining clearances
- Increased competition
- Lack of qualified personnel for implementation
- Limited enforcement of regulations

The NCSC's Evaluated Products List (EPL) is also judged inadequate by some vendors. One vendor official, William Norvell of Hughes, was quoted as saying that secure systems often fail "not because they do not meet regulations, but because they fail to meet unspecified operational requirements."

C
Vendor Contracting Views

1. Preferred Contractors

Vendors were asked to indicate which type of company they believe federal agencies will prefer, in rank order of preference. As illustrated in Exhibit V-12, industry respondents believe that the use of systems integrators is most preferable to the agencies. Many vendors are currently offering or planning to offer systems integration services.

EXHIBIT V-11

Vendor Perceptions of Agency Preferences for Security Contractors

Type of Contractor	Vendor Rank*
Systems Integrator	1
Hardware Vendor	2
Software Manufacturers	3
Professional Services Firm	4
Aerospace Divisions	5
Not-for-Profit	6
Foreign Manufacturers	7

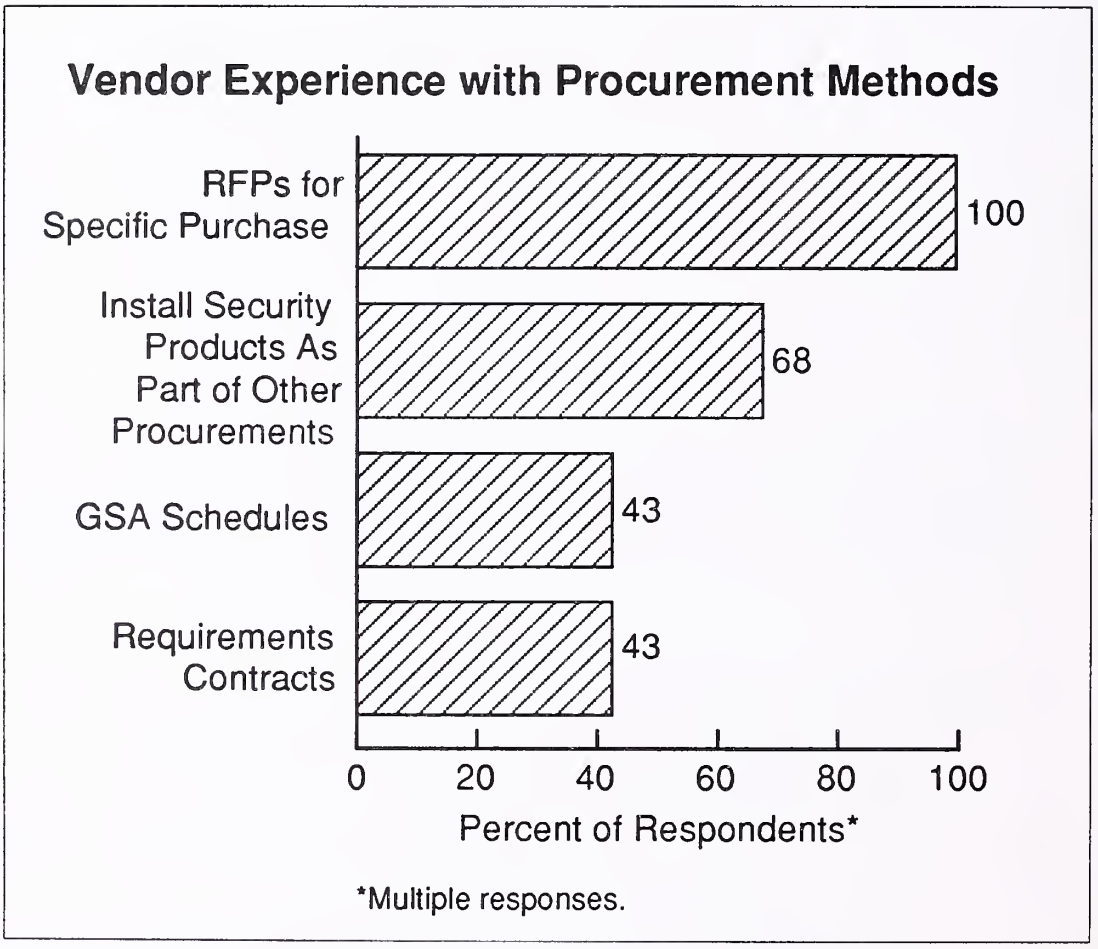
*Rank based on average score for each contractor type.

Vendors also believe that agencies prefer to use the services of hardware and software companies to undertake implementation of security programs. These vendors appear to be a logical choice, since they can supply the right match of skills and resources required for many federal projects and are already strong players in the market. There was no indication of agency preferences for 8(a) and other minority businesses.

2. Vendor Experience with Procurement Methods

Vendors were queried about which procurement methods they have responded to in marketing their computer security products and services to the federal government. Results are shown in Exhibit V-12. All of the industry representatives surveyed have responded to RFPs from agencies. Over two-thirds of the respondents have installed security products and services as part of other procurements. A smaller share of vendors (43%) participate on GSA Schedules. This method of providing products to the government is likely to increase over the next two to five years. At present, there are very few requirements contracts for computer security products and services.

EXHIBIT V-12

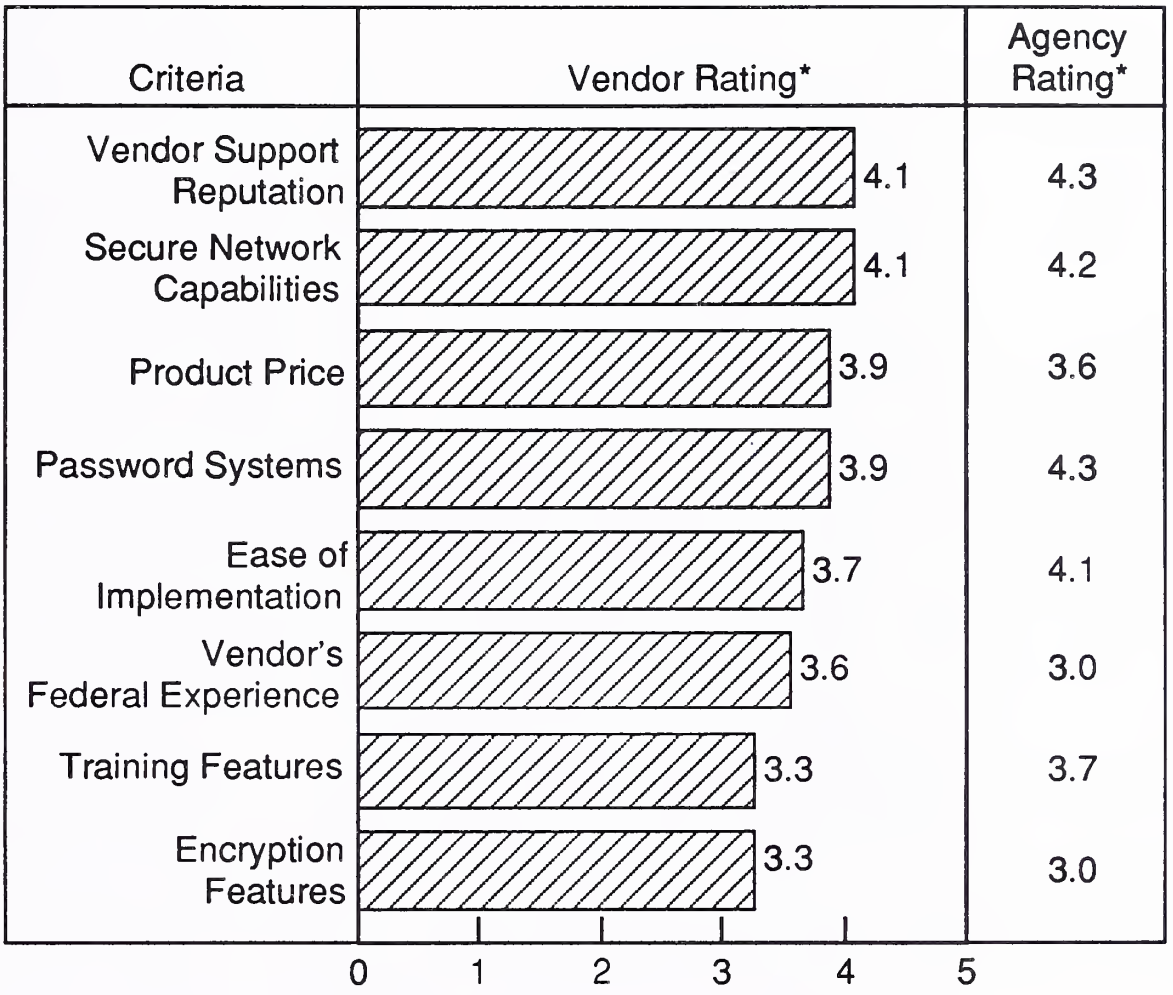


3. Vendor Selection Criteria

Vendors need to better understand and respond to the criteria utilized by the government in selecting a winning vendor for computer security products and services. As shown in Exhibit V-13, industry respondents consider the vendor's support reputation the number-one selection criterion. This suggests the importance of service in meeting federal security needs. The agencies concur with the vendor perceptions. The two respondent groups also gave similarly high ratings for the importance of secure network capabilities.

EXHIBIT V-13

Vendor Selection Criteria



*Rating: 1 = not important, 5 = very important.

The agencies indicated greater importance of password systems, ease of implementation, and training features than did the industry vendors. This may arise from agencies having a user perspective. The industry respondents placed more importance on federal experience than was apparent to the agencies. However, both groups are in some agreement on the moderate range of importance for product price and encryption features.

D
Teaming Patterns

Teaming efforts in the federal market are becoming more frequent in order to respond to the terms and conditions of many agency RFPs. Most vendors view their teaming relationships as moderately successful, with the average rating at 3.7. This suggests that vendors may need to improve their teaming efforts.

Exhibit V-14 lists the respondents' rating of their levels of success. Over one-third (36%) selected a rating level of three, indicating moderate success. Another 20% each indicated a rating of either 4 or 5, which suggests a considerably high degree of satisfaction with their current teaming experiences.

EXHIBIT V-14

Success Level of Vendor Teaming Relationships

Success Level*	Percent of Respondents
1	0
2	4
3	36
4	20
5	20
No Response/ No Teaming Experience	20

Note: Overall teaming success rating: 3.7, based on a 1 to 5 scale.

*1 = not successful at all, 5 = extremely successful.

Exhibit V-15 lists vendor types cited by the industry respondents as their most frequent teaming partners. Software and hardware vendors combined are mentioned most often as team members. They are chosen for their ability to provide the appropriate skills and resources required for many federal projects and their understanding of the existing computer systems.

A close second place for mention as partners were systems integrators. As noted earlier, many of the companies surveyed are already performing systems integration functions or will be in the future. Also, in the next few years, teaming with the Tempest hardware firms and small market niche companies may increase as security requirements to be implemented call upon the specialized expertise of these companies.

Teaming activities present their own set of related vendor concerns and issues. In previous INPUT studies of teaming among vendors, the industry respondents recognized the need for more cooperation and communication with teaming partners. The vendors also noted their own shortcomings in not fully identifying all the requirements of a program early enough in the planning process. If these problems are overcome by computer security vendors, this better planning could aid in developing stronger teaming of companies that are more suitably matched.

EXHIBIT V-15

Preferred Teaming Partner for Security Contracts

Vendor Type	Percent of Respondents
Hardware and Software Vendors	27
Systems Integrators	23
Hardware Manufacturers and Systems Integrators	14
Hardware Manufacturers and Professional Services Firms	9
Software Firms	9
Tempest Hardware Firms	9
Small Market Niche Companies	9

Industry respondents have also mentioned in previous studies the need to improve the marketing of their team members' products as well as increasing their reliance on standard products. In addition, teaming efforts should focus on improving delivery schedules and product prices. These suggestions appear relevant to the federal computer security market.

E
Vendor Performance

1. Ratings of Vendor Performance

Both agency and vendor respondents were asked to evaluate agency perceptions of vendor performance characteristics. Exhibit V-16 compares the vendors' and agencies' ratings of these characteristics.

EXHIBIT V-16

Comparative Ratings of Vendor Performance

Characteristic	Vendor Rating*	Agency Rating*
Hardware Offered	3.5	3.1
Encryption Experience	3.4	3.3
Successful Implementation	3.3	3.3
Training Experience	3.1	3.3
Staff Experience	3.1	3.3
Software Offered	3.0	3.3
Price	3.0	3.2
Support Experience	3.0	3.2
Delivery Schedule	2.7	3.1

*Rating: 1 = definitely not satisfactory, 5 = outstanding performance.

Some differences in opinion appear to exist between the two respondent groups. The characteristic rated most satisfactory by the vendors was hardware offered, whereas the agencies experienced lower levels of satisfaction from the products acquired. There are minor differences between the responses from the agencies and vendors on most other characteristics. However, for their adherence to delivery schedules, the industry respondents rated industry performance at only 2.7, while agencies averaged a 3.1 rating for this characteristic. This suggests that vendors are already aware of their need to improve timely availability of products in line with the agencies' perceptions of successful vendors.

2. Suggested Improvements to Products and Services

Industry respondents were asked what improvements vendors could make to their products and services over the next five years to make them more valuable to the federal market. Exhibit V-17 lists the responses.

The replies varied as a result of different types and levels of experience vendors have encountered with federal agencies. Improvements to the user friendliness of security products and services were mentioned by the largest percentage of the respondents. The improvements, along with the increased awareness and training of federal personnel/users, could help to promote more effective use of security safeguards.

EXHIBIT V-17

Suggested Improvements for Security Products and Services

Suggestion	Percent of Respondents
Improve User Friendliness	21
Offer a Broad Range of Interoperable Systems	18
Improve Software Security Features	18
Other	14
Lower the Price	11
Standardize Security on Off-the-Shelf Technology	11
Shorten Cycle of Validation/Certification	7

The suggested improvements to interoperability of systems and improved software features are similar to suggestions made by the agency respondents. Some vendors noted that standardizing with off-the-shelf technology would improve their business relationships with the federal government, as agencies are seeking cost-effective solutions to security requirements.

Only a few vendors acknowledged possible improvements to the lengthy validation and certification processes. These processes are essential to the development of products in order to comply with a full range of rigid requirements and standards.

Other suggestions made by the industry respondents include:

- Improved training
- Development of nonproprietary architecture
- Improved compliance with federal market demand
- Improved accuracy in advertisements of product capabilities

F
Trends

1. Technology Trends

Industry representatives were asked to identify technological factors that would affect the federal government's computer security requirements. The factors named most frequently are listed in Exhibit V-18.

The vendors frequently noted that additional and more complex networking capabilities will increase the computer system access control requirements and also require the development of security safeguards for information storage and transmission. Agency respondents also selected expanded networks as the top-ranked technological factor to affect the federal computer market over the next few years.

The increased use of workstations at agencies for end-user computing has necessitated that industry bring secure technology down to the workstation level. Products such as SecureWare's Compartmented Mode Workstation (CMW) and Contel's Secure Workstations Project already show the efforts of some firms to move into this segment of the federal marketplace. Contel is installing 1,200 high-end Sun Microsystems workstations at OSD, under a project called the Office Automation Secure Information System (OASIS). Further, under its Compartmented Mode Workstation procurement, the DIA is buying secure workstations from Harris, Digital, and IBM.

EXHIBIT V-18

Vendor Ranking of Technological Factors Affecting Computer Security

Factor	Vendor Rank*
Increase in Networking Capabilities	1
Developments in Workstation Environment	2
Increase in Distributed Processing	3
Advancements and Increased Use of RDBMS	4
Standardization Efforts	4
Migration of Open Systems	4
Advancements in Hardware to Incorporate Security Features	5
Implementation of UNIX/POSIX	5
Developments in Telecommunications	6

*Rank based on frequency of mention by respondents.

Distributed processing is also contributing to agencies' increasing their security requirements. The development of programmable intelligence in order to perform data processing functions more effectively through computers and terminals arranged in a telecommunications network will result in a greater agency need for encryption of data transmission lines.

As shown in Exhibit V-18, several technological factors tied for fourth place in frequency of mention. Many of the software vendors, as well as other companies surveyed, noted that relational data base management systems (RDBMS) will impact the market. This market niche in general is already highly competitive.

Standardization efforts will continue to play a major role in the federal computer security market. In some cases, vendors are jointly working with federal organizations in developing standards that incorporate commercial developments and previous computer security expertise.

Intersystem compatibility and implementation of OSI will require that vendor security products contribute to the flexibility and adaptability of governmental information systems. Open systems will require security in various levels of the OSI model. The NIST Computer Systems Lab has been working with vendors to address the security issues of OSI.

Advances in hardware, implementation of UNIX/POSIX, and developments in telecommunications were technologies cited by both vendor and industry respondents as having an influence on federal computer security requirements and implementation. Many vendors acknowledged that federal agencies need to go beyond just physical and software security solutions, and were positioning themselves to offer the hardware to support agency applications in a secure environment in the future. POSIX requires application portability security and, along with UNIX, has gained a government-wide foothold.

Telecommunications developments such as fiber optics will impact the security products to be developed by vendors. Additional methods of communicating between systems can extend the security features needed for the agency system. In general, any product or service that enhances interoperability also increases the need for security.

The NIST Technical Security Program plays an active role in the utilization of new technologies to enhance the security of federal computer systems. NIST personnel are currently working on a variety of technical issues that will be prominent in the 1990s. These include:

- POSIX
- Network security
- Data encryption
- Key management
- Message authentication
- Network access control
- ISDN
- Anti-virus activities

NIST releases policy statements and technical publications in order to disseminate the technical information compiled by the various divisions of the National Computer Systems Laboratory.

2. Budgetary Constraints

As shown in Exhibit V-19, industry respondents expressed varying opinions as to the effects of federal budget constraints on the federal computer security market. The vendors view delays in implementation, funding cuts and downsizing of security efforts as the main effects. Twenty-one percent of the industry respondents viewed the effects as minimal due to the decreasing product price. However, many industry products are still considered costly by government agencies. As indicated in Chapter III, INPUT does not concur with this viewpoint. INPUT considers budget constraints to be the dominant negative market factor.

EXHIBIT V-19

Impact of Budgetary Constraints

Impact	Percent of Respondents
Delays Implementation of Security Features	25
Minimal Impact/Decreasing Product Prices	21
Security Low Priority/Cut from Budget	18
Other/No Response	18
Significant Impact	11
Downsize Security Efforts	7

Budget cuts will hinder the security training and implementation phases at many agencies, thus initially slowing market demand for some products and services. Furthermore, cancellation or reduced funding of a major systems procurement can result in a lengthy procurement process and potential loss of acquisitions for the security component of the proposed system.

3. Market Trends

The market factors that vendors believe will impact the federal computer security market were numerous and varied. INPUT lists the responses in order of frequency mentioned in Exhibit V-20.

EXHIBIT V-20

Market Trends Impacting the Computer Security Market

Factor	Rank*
Availability of Security Products	1
Regulation/Computer Security Act	2
Mergers/Joint Ventures with Hardware and Software Firms	3
Privacy Issues	4

*Rank based on frequency of mention by respondents.

The marketplace is expected to change over the next two to five years as an influx of products occurs. Additional UNIX-based products, secure workstations, and encryption systems will be competing for market share with existing products.

Federal regulations and the Computer Security Act will continue to provide guidance and direction to the industry. The proposed anti-virus legislation, fraud prevention, and other security-related agency directives give additional weight to the importance of computer security for federal information systems and may spark greater demand for products and services.

As in other segments of the information industry, the federal computer security marketplace is experiencing an increase in mergers and joint ventures. Economic conditions dictate that stronger competitors buy out their weaker competition. Also, smaller niche companies are targets of mergers/acquisitions by larger firms that are interested in more quickly marketing the specialized products. Joint ventures have become common between hardware and software firms in order to respond to more complex and all-inclusive government RFPs.

Many of the privacy issues related to computer security still remain unresolved. The government has information that, although nonclassified, is still only suitable for restrictive disclosure due to the protection of individuals' or corporations' rights to privacy. Legislation is pending that will reinforce privacy rights and inflict greater punishments for security violations.

4. Impact of Government Policy Agencies

Industry respondents were surveyed to obtain their views on how government policies and regulations from GSA, NIST, and NSA will impact the federal computer security market in the future. The vendors gave a variety of responses that can be grouped into two general areas: the responsibilities of each specific agency studied, and the resulting impact on the federal computer security market. The following outline conveniently summarizes the comments received and supports INPUT's earlier discussion of policies and regulations, found in Chapter III.

A. National Institute of Standards and Technology (NIST)
   1. Areas of Responsibility
      - Develop standards (i.e., DES, POSIX, Network Security)
      - Provide guidance and training
      - Operate within internal agreement with NSA on policy development
      - Assist agencies to achieve C2 by 1992

   2. Impact on Federal Computer Security Market
      - Develops additional requirements
      - Centers more attention on standards than security
      - Increases awareness/compliance
      - Promotes implementation of off-the-shelf technology

B. National Security Agency (NSA)
   1. Areas of Responsibility
      - Define security protocols
      - Monitor product evaluation/certification process
      - Concentrate efforts in DoD and classified areas
      - Assist with technical problems and security issues related to national security

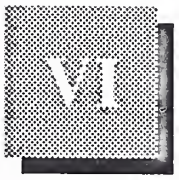
   2. Impact on Federal Computer Security Market
      - Need to simplify product evaluation process
      - Develops additional access control requirements
      - Need to improve coordination efforts with industry and NIST
      - Increases agency use of security products

C. General Services Administration (GSA)
   1. Areas of Responsibility
      - Evaluate A, B, and C security categories to promote more effective use of hardware and software
      - Establish procurement regulations
      - Assist with establishing federal security policies
      - Mandate security planning for agency DPAs (Delegations of Procurement Authority)

2. Impact on Federal Computer Security Market
   - Influences size of procurements
   - Compounds problem of MLS/interoperability
   - Need stricter enforcement of standards
   - Minimal impact on security
   - Increases agency use of security products

Industry respondents viewed the activities and assistance provided by each of these agencies as mostly beneficial. However, they expressed some frustration as a result of conflicts in attempting to comply with a variety of standards and requirements developed by the policy-formulating agencies studied. The comments received by the vendors are similar to those of the agency respondents summarized in Exhibit IV-22. Both groups of respondents view NSA as taking the leading role in product evaluation and GSA as having the least impact overall.

In the future, new legislation will likely clarify the roles of the various oversight agencies. There are currently too many ambiguities in responsibilities, leaving both agencies and vendors somewhat bewildered about who is really in charge.



Key Opportunities

This section describes specific opportunities in the federal information technology market.

Although this opportunity list is not all-inclusive, it includes major programs typical of the federal market.

This list of opportunities becomes smaller after FY 1992 because new programs have not yet been identified or initially approved by the responsible agency. Subsequent issues of this report and the INPUT Procurement Analysis Reports will include additional programs and detailed program information for FY 1992 - FY 1997.

A
Present and Future Programs

New information technology programs larger than $1-2 million are listed in at least one of the following federal government documents:

- OMB/GSA Five-Year Plan, which is developed from agency budget requests submitted in compliance with OMB Circular A-ll
- Agency long-range information resource plans developed to meet the reporting requirements of the Paperwork Reduction Reauthorization Act of 1986
- Agency annual operating budget requests submitted to congressional oversight and appropriations committees based on the OMB A-ll information
- *Commerce Business Daily* for specific opportunities for qualifications as a bidder, and invitations to submit a bid in response to an RFP or RFQ
- Five-Year Defense Plan, which is not publicly available, and the supporting documentation of the separate military departments and agencies

- Classified program documentation available only to qualified DoD contractors

Opportunities related to computer security may not be specifically identified as such in these documents. Information technology planning documents usually identify mission requirements to be met by specific programs, rather than methods for meeting those requirements. Computer security requirements are increasingly becoming incorporated into procurements as part of the overall system requirements rather than as a separate procurement. Also, with increased emphasis on federal computer security, security is being seen more frequently as a system requirement in RFPs.

All funding proposals are based on cost data of the year submitted, with inflation factors dictated by the Administration as part of its fiscal policy, and are subject to revision, reduction, or spread to future years in response to congressional direction. Some additional reductions will be likely in FY 1992 and beyond, due to the tightening of the Department of Defense budget.

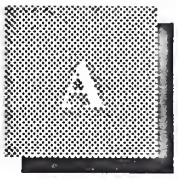
B

Computer Security Opportunities by Agency

Agency/Program	PAR Preference	Approximate RFP Date	FY92-FY97 Funding (Est. $000)
Air Force			
Air Force Information Publishing Service	V-01-152	3/1/92	20,000
Commerce Hardware/Software	V-02-051	4/1/92	2,000,000
Defense			
Defense Information System Network	V-04G-009	1/1/93	*
RISC Technology Workstation	V-04H-003	*	*
Joint Worldwide Intelligent Communications System	V-04H-004	6/1/92	*
Federal Communications Commission			
Information System Modernization	VIII-34-001	6/1/92	*
Justice			
FBI Field Office Information Management System	VII-10-002	10/1/93	*
Computer Applications Communications Network	VII-10-009	10/1/93	*

Agency/Program	PAR Preference	Approximate RFP Date	FY92-FY97 Funding (Est. $000)
Personal Workstation Acquisition	VII-10-35	4/1/92	50,000
Local-Area Network Equipment and Software	VII-10-37	3/30/92	50,000
Treasury			
Service Center Support System	VII-12-065	4/1/92	2,200,000
Treasury Communications System	VII-12-077	3/31/92	150,000

*Unknown



Federal Computer Security Market Interview Profiles

A

Federal Agency Respondent Profile

Recent interviews were conducted (in February 1992) with two NIST Computer Systems Lab Security executives. The interviews were conducted on-site at NIST headquarters.

Interviews in 1990 were conducted by telephone and mail. The respondents interviewed included administrative policy officials, contracting officers, and program managers in the following agencies:

Department of the Air Force

Department of the Army

Department of Commerce

Defense Technical Information Center

Department of Energy

General Accounting Office

Department of Health and Human Services

- Food and Drug Administration
- Public Health Service

Department of Housing and Urban Development

Department of the Interior

Department of Justice

- U.S. Marshals Service

NASA

Department of the Navy

- Naval Supply Systems Command
- Naval Weapons Center

Office of the Secretary of Defense

Smithsonian Institute

Supreme Court of the United States

Department of Treasury

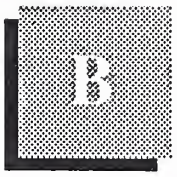
- Internal Revenue Service

B
Vendor Respondent Profile

INPUT did not conduct industry interviews for this revision. In 1990, INPUT contacted a representative sample of contractors that provided or planned to provide computer security products and services to the federal government.

Job classifications among individual vendor respondents included marketing, program managers, and administrative executives.

Interviews with vendor personnel were conducted by telephone and by mail.



Definition of Terms

A Introduction

INPUT's *Definition of Terms* provides the framework for all of INPUT's market analyses and forecasts of the information services industry. It is used for all U.S. programs. The structure defined in Exhibit B-1 is also used in Europe and for the worldwide forecast.

One of the strengths of INPUT's market analysis services is the consistency of the underlying market sizing and forecast data. Each year INPUT reviews its industry structure and makes changes if they are required. When changes are made they are carefully documented and the new definitions and forecasts reconciled to the prior definitions and forecasts. INPUT clients have the benefit of being able to track market forecast data from year to year against a proven and consistent foundation of definitions.

For 1992 INPUT has incorporated customer services (hardware maintenance) into the information services industry structure. Equipment service becomes the ninth delivery mode used by INPUT to segment and analyze this industry.

In addition, some new areas are being researched during 1992 as part of the outsourcing area and may result in future changes to the industry structure. These areas of research are discussed in Section B 5 of this document.

B

Overall Definitions and Analytical Framework

1. Information Services

Information Services are computer/telecommunications-related products and services that are oriented toward the development or use of information systems. Information services typically involve one or more of the following:

- Processing of specific applications using vendor-provided systems (called *Processing Services*)
- A combination of hardware, packaged software and associated support services which will meet a specific application processing need (called *Turnkey Systems*)
- Packaged software products, either systems software or applications software products (called *Software Products*)
- People services that support users in developing and operating their own information systems (called *Professional Services*)
- Bundled combinations of products and services where the vendor assumes total responsibility for the development of a custom solution to an information systems problem (called *Systems Integration*)
- Services that provide operation and management of all or a significant part of a user's information systems functions under a long-term contract (called *Systems Operations*)
- Services associated with the delivery of information in electronic form—typically network-oriented services such as value-added networks, electronic mail and document interchange, on-line data bases, on-line news and data feeds, etc. (called *Network Services*)
- Services that support the operation of computer hardware and resident systems software (called *Equipment Services*)

In general, the market for information services does not involve providing equipment to users. The exception is where the equipment is bundled as part of an overall service offering such as a turnkey system, a systems operations contract, or a systems integration project.

The information services market also excludes pure data transport services (i.e., data or voice communications circuits). However, where information transport is associated with a network-based service (e.g., EDI or VAN services), or cannot be feasibly separated from other bundled services (e.g., some systems operations contracts), the transport costs are included as part of the services market.

The analytical framework of the information services industry consists of the following interacting factors: overall and industry-specific business environment (trends, events and issues); technology environment; user information system requirements; size and structure of information services markets; vendors and their products, services and revenues; distribution channels; and competitive issues.

2. Market Forecasts/User Expenditures

All information services market forecasts are estimates of *User Expenditures* for information services. When questions arise about the proper place to count these expenditures, INPUT addresses them from the user's viewpoint: expenditures are categorized according to what users perceive they are buying.

By focusing on user expenditures, INPUT avoids two problems which are related to the distribution channels for various categories of services:

- Double counting, which can occur by estimating total vendor revenues when there is significant reselling within the industry (e.g., software sales to turnkey vendors for repackaging and resale to end users)

- Missed counting, which can occur when sales to end users go through indirect channels such as mail order retailers

Captive Information Services User Expenditures are expenditures for products and services provided by a vendor that is part of the same parent corporation as the user. These expenditures are not included in INPUT forecasts.

Non-captive Information Services User Expenditures are expenditures that go to vendors that have a different parent corporation than the user. It is these expenditures which constitute the information services market analyzed by INPUT and that are included in INPUT forecasts.

3. Delivery Modes

Delivery Modes are defined as specific products and services that satisfy a given user need. While *Market Sectors* specify *who* the buyer is, *Delivery Modes* specify *what* the user is buying.

Of the nine delivery modes defined by INPUT, six are considered primary products or services:

- *Processing Services*
- *Network Services*
- *Professional Services*
- *Applications Software Products*
- *Systems Software Products*
- *Equipment Services*

The remaining three delivery modes represent combinations of these products and services, bundled together with equipment, management and/or other services:

- *Turnkey Systems*
- *Systems Operations*
- *Systems Integration*

Section C describes the delivery modes and their structure in more detail.

4. Market Sectors

Market Sectors or markets are groupings or categories of the users who purchase information services. There are three types of user markets:

- *Vertical Industry* markets, such as Banking, Transportation, Utilities, etc. These are called "industry-specific" markets.

- *Functional Application* markets, such as Human Resources, Accounting, etc. These are called "cross-industry" markets.

- *Other* markets, which are neither industry- nor application-specific, such as the market for systems software products and much of the on-line data base market.

Specific market sectors used by INPUT are defined in Section E, below.

5. Outsourcing

The changes in the information services area towards longer term client-vendor relationships has created a number of new types of *outsourcing* relationships. In addition to the nine delivery modes, INPUT will be conducting research during 1992 in each of the areas defined below. Based on this research, INPUT will review and may change its information services industry structure for 1992.

- Outsourcing - The contracting of all or a major part of an information systems process to an external vendor on a long-term basis. The vendor takes responsibility for the performance of the process.

- Outsourcing can include any or all of the following elements:
  - Processing Operations - The vendor is responsible for managing and operating the client's computer systems.
  - Network Operations - The vendor assumes full responsibility for the client's data communications systems. This may also include the voice communications of the client.
  - Applications Maintenance - The vendor has full responsibility for maintaining the applications software that the vendor uses as part of its business operations.
  - Applications Management - Not only does the vendor maintain and upgrade the applications software for the client, but also develops and implements new software as the need arises.
  - Desktop Services - The vendor assumes responsibility for the deployment, maintenance and connectivity between the PCs in the client organization. The service may also include performing the help desk function.

C
Delivery Modes and Submodes

Exhibit B-1 provides the overall structure of the information services industry as defined and used by INPUT. This section of *Definition of Terms* provides definitions for each of the delivery modes and their submodes or components.

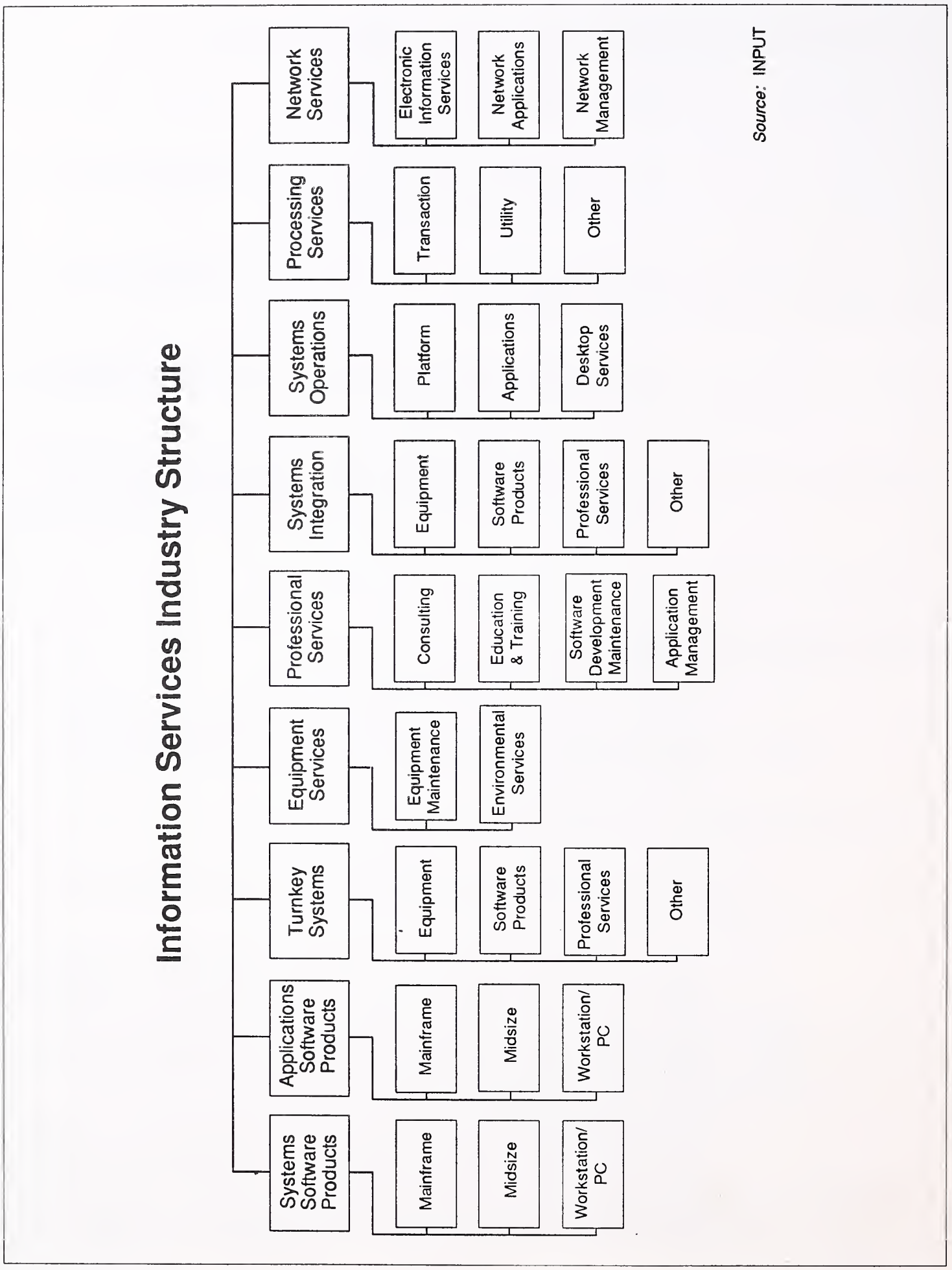
1. Software Products

INPUT divides the software products market into two delivery modes: systems software and applications software.

The two delivery modes have many similarities. Both involve user purchases of software packages for in-house computer systems. Included are both lease and purchase expenditures, as well as expenditures for work performed by the vendor to implement or maintain the package at the user's sites. Vendor-provided training or support in operation and use of the package, if bundled in the software pricing, is also included here.

Expenditures for work performed by organizations other than the package vendor are counted in the professional services delivery mode. Fees for work related to education, consulting, and/or custom modification of software products are counted as professional services, provided such fees are charged separately from the price of the software product itself.

EXHIBIT B-1



a. Systems Software Products

Systems software products enable the computer/communications system to perform basic machine-oriented or user interface functions. INPUT divides systems software products into three submodes.

- *Systems Control Products* - Software programs that function during application program execution to manage computer system resources and control the execution of the application program. These products include operating systems, emulators, network control, library control, windowing, access control, and spoolers.

- *Operations Management Tools* - Software programs used by operations personnel to manage the computer system and/or network resources and personnel more effectively. Included are performance measurement, job accounting, computer operation scheduling, disk management utilities, and capacity management.

- *Applications Development Tools* - Software programs used to prepare applications for execution by assisting in designing, programming, testing, and related functions. Included are traditional programming languages, 4GLs, data dictionaries, data base management systems, report writers, project control systems, CASE systems and other development productivity aids. Also included are system utilities (e.g., sorts) which are directly invoked by an applications program.

INPUT also forecasts the systems software products delivery mode by platform level: mainframe, minicomputer and workstation/PC.

b. Applications Software Products

Applications software products enable a user or group of users to support an operational or administrative process within an organization. Examples include accounts payable, order entry, project management and office systems. INPUT categorizes applications software products into two submodes.

- *Industry-Specific Applications Software Products* - Software products that perform functions related to fulfilling business or organizational needs unique to a specific industry (vertical) market and sold to that market only. Examples include demand deposit accounting, MRPII, medical record keeping, automobile dealer parts inventory, etc.

- *Cross-Industry Applications Software Products* - Software products that perform a specific function that is applicable to a wide range of industry sectors. Examples include payroll and human resource systems, accounting systems, word processing and graphics systems, spreadsheets, etc.

INPUT also forecasts the applications software products delivery mode by platform level: mainframe, minicomputer and workstation/PC.

2. Turnkey Systems

A turnkey system is an integration of equipment (CPU, peripherals, etc.), systems software, and packaged or custom application software into a single product developed to meet a specific set of user requirements. Value added by the turnkey system vendor is primarily in the software and support services provided. Most CAD/CAM systems and many small business systems are turnkey systems. Turnkey systems utilize standard computers and do not include specialized hardware such as word processors, cash registers, process control systems, or embedded computer systems for military applications.

Computer manufacturers (e.g., IBM or DEC) that combine software with their own general-purpose hardware are not classified by INPUT as turnkey vendors. Their software revenues are included in the appropriate software category.

Most turnkey systems are sold through channels known as value-added resellers.

- *Value-Added Reseller (VAR):* A VAR adds value to computer hardware and/or software and then resells it to an end user. The major value added is usually applications software for a vertical or cross-industry market, but also includes many of the other components of a turnkey systems solution, such as professional services.

Turnkey systems have three components:

- Equipment - computer hardware supplied as part of the turnkey system
- Software products - prepackaged systems and applications software products
- Professional services - services to install or customize the system or train the user, provided as part of the turnkey system sale

3. Processing Services

This delivery mode includes three submodes: transaction processing, utility processing, and "other" processing services.

- *Transaction Processing* - Client uses vendor-provided information systems—including hardware, software and/or data networks—at the vendor site or customer site to process transactions and update client data bases. Transactions may be entered in one of four modes:

- *Interactive* - Characterized by the interaction of the user with the system for data entry, transaction processing, problem solving and report preparation: the user is on-line to the programs/files stored on the vendor's system.

- *Remote Batch* - Where the user transmits batches of transaction data to the vendor's system, allowing the vendor to schedule job execution according to overall client priorities and resource requirements.

- *Distributed Services* - Where users maintain portions of an application data base and enter or process some transaction data at their own site, while also being connected through communications networks to the vendor's central systems for processing other parts of the application.

- *Carry-in Batch* - Where users physically deliver work to a processing services vendor.

• *Utility Processing* - Vendor provides basic software tools (language compilers, assemblers, DBMSs, graphics packages, mathematical models, scientific library routines, etc.), generic applications programs and/or data bases, enabling clients to develop their own programs or process data on the vendor's system.

• *Other Processing Services* - Vendor provides service—usually at the vendor site—such as scanning and other data entry services, laser printing, computer output microfilm (COM), CD preparation and other data output services, backup and disaster recovery, etc.

4. Systems Operations

Systems operations was a new delivery mode introduced in the 1990 Market Analysis and Systems Operations programs. It was created by taking the Systems Operations submode out of both Processing Services and Professional Services. For 1992 the submodes have been defined as follows.

Systems operations involves the operation and management of all or a significant part of the user's information systems functions under a long-term contract. These services can be provided in either of two distinct submodes where the difference is whether the support of applications, as well as data center operations, is included.

• *Platform systems operations* - The vendor manages and operates the computer systems, often including telecommunications networks, without taking responsibility for the user's application systems.

- *Applications systems operations* - The vendor manages and operates the computer systems, often including telecommunications networks, and is also responsible for maintaining, or developing and maintaining, the user's application systems.

In the federal government market, systems operation services are also defined by equipment ownership with the terms "COCO" (Contractor-Owned, Contractor-Operated), and "GOCO" (Government-Owned, Contractor-Operated).

The ownership of the equipment, which was the previous basis for the systems operations submodes, is no longer considered critical to the commercial market. Most of the market consists of systems operations relationships using vendor-owned hardware. What is now critical is the breadth of the vendor/client relationship as it expands beyond data center management to applications management.

Systems operations vendors now provide a wide variety of services in support of existing information systems. The vendor can plan, control, provide, operate, maintain and manage any or all components of the user's information systems (equipment, networks, systems and/or applications software), either at the client's site or the vendor's site. Systems operations can also be referred to as "resource management" or "facilities management."

5. Systems Integration (SI)

Systems integration is a vendor service that provides a complete solution to an information system, networking or automation requirement through the custom selection and implementation of a variety of information system products and services. A systems integrator is responsible for the overall management of a systems integration contract and is the single point of contact and responsibility to the buyer for the delivery of the specified system function, on schedule and at the contracted price.

To be included in the information services market, systems integration projects must involve some application processing component. In addition, the majority of cost must be associated with information systems products and/or services.

- *Equipment* - Information processing and communications equipment required to build the systems solution. This component may include custom as well as off-the-shelf equipment to meet the unique needs of the project. The systems integration equipment category excludes turnkey systems by definition.

- *Software products* - Prepackaged applications and systems software products.

- *Professional services* - The value-added component that adapts the equipment and develops, assembles, or modifies the software and hardware to meet the system's requirements. It includes all of the professional services activities required to develop, and if included in the contract, operate an information system, including consulting, program/project management, design and integration, software development, education and training, documentation, and systems operations and maintenance.

- *Other services* - Most systems integration contracts include other services and product expenditures that are not easily classified elsewhere. This category includes miscellaneous items such as engineering services, automation equipment, computer supplies, business support services and supplies, and other items required for a smooth development effort.

Systems integrators perform, or manage others who perform, most or all of the following functions:

- Program management, including subcontractor management
- Needs analysis
- Specification development
- Conceptual and detailed systems design and architecture
- System component selection, modification, integration and customization
- Custom software design and development
- Custom hardware design and development
- Systems implementation, including testing, conversion and post-implementation evaluation and tuning
- Life cycle support, including
  - System documentation and user training
  - Systems operations during development
  - Systems maintenance

6. Professional Services

This category includes three submodes: consulting, education and training, and software development.

- *Consulting:* Services include management consulting (related to information systems), information systems consulting, feasibility analysis and cost-effectiveness studies, and project management assistance. Services may be related to any aspect of the information system, including equipment, software, networks and systems operations.

- *Education and Training:* Products and services related to information systems and services for the professional and end user, including computer-aided instruction, computer-based education, and vendor instruction of user personnel in operations, design, programming, and documentation.

- *Software Development:* Services include user requirements definition, systems design, contract programming, documentation, and implementation of software performed on a custom basis. Conversion and maintenance services are also included.

7. Network Services

Network services typically include a wide variety of network-based functions and operations. Their common thread is that most of these functions could not be performed without network involvement. Network services is divided into two submodes: *Electronic Information Services,* which involve selling information to the user, and *Network Applications,* which involve providing some form of enhanced transport service in support of a user's information processing needs.

a. Electronic Information Services

Electronic information services are data bases that provide specific information via terminal- or computer-based inquiry, including items such as stock prices, legal precedents, economic indicators, periodical literature, medical diagnosis, airline schedules, automobile valuations, etc. The terminals used may be computers themselves, such as communications servers or personal computers. Users typically inquire into and extract information from the data bases. Although users may load extracted data into their own computer systems, the electronic information vendor provides no data processing or manipulation capability and the users cannot update the vendor's data bases.

The two kinds of electronic information services are:

- *On-line Data Bases* - Structured, primarily numerical data on economic and demographic trends, financial instruments, companies, products, materials, etc.

- *News Services* - Unstructured, primarily textual information on people, companies, events, etc.

While electronic information services have traditionally been delivered via networks, there is a growing trend toward the use of CD ROM optical disks to support or supplant on-line services, and these optical disk-based systems are included in the definition of this delivery mode.

b. Network Applications

Value-Added Network Services (VAN Services) - VAN services are enhanced transport services which involve adding such functions as automatic error detection and correction, protocol conversion, and store-and-forward message switching to the provision of basic network circuits.

While VAN services were originally provided only by specialized VAN carriers (Tymnet, Telenet, etc.), today these services are also offered by traditional common carriers (AT&T, Sprint, etc.). Meanwhile, the VAN carriers have also branched into the traditional common carriers' markets and are offering unenhanced basic network circuits as well.

INPUT's market definition covers VAN services only, but includes the VAN revenues of all types of carriers. The following are examples of VAN services.

- *Electronic Data Interchange (EDI)* - Application-to-application exchange of standardized business documents between trade partners or facilitators. This exchange is commonly performed using VAN services. Specialized translation software is typically employed to convert data from organizations' internal file formats to EDI interchange standards. This software may be provided as part of the VAN service or may be resident on the organization's own computers.

- *Electronic Information Exchange (EIE)* - Also known as electronic mail (E-mail), EIE involves the transmission of messages across an electronic network managed by a services vendor, including facsimile transmission (FAX), voice mail, voice messaging, and access to Telex, TWX, and other messaging services. This also includes bulletin board services.

- *Other Network Services* - This segment contains videotex and pure network management services. Videotex is actually more a delivery mode than an application. Its prime focus is on the individual as a consumer or in business. These services provide interactive access to data bases and offer the inquirer the ability to send as well as receive information for such purposes as home shopping, home banking, travel reservations, and more.

  Network management services included here must involve the vendor's network and network management systems as well as people. People-only services are included in professional services that involve the management of networks as part of the broader task of managing a user's information processing functions are included in systems operations.

8. Equipment Services

The equipment services delivery mode includes two submodes. Each deals with the support and maintenance of computer equipment operations.

- *Equipment Maintenance* - Services provided to repair, diagnose problems and provide preventive maintenance both on-site and off-site. The costs of parts, media and other supplies are excluded. These services are typically provided on a contract basis.

- *Environmental Services* - Composed of equipment- and data center-related special services such as cabling, air conditioning and power supply, equipment relocation and similar services.

D
Hardware/Hardware Systems

Hardware - Includes all computer and telecommunications equipment that can be separately acquired with or without installation by the vendor and not acquired as part of an integrated system.

- *Peripherals* - Includes all input, output, communications, and storage devices (other than main memory) that can be connected locally to the main processor, and generally cannot be included in other categories such as terminals.

- *Input Devices* - Includes keyboards, numeric pads, card readers, light pens and track balls, tape readers, position and motion sensors, and analog-to-digital converters.

- *Output Devices* - Includes printers, CRTs, projection television screens, micrographics processors, digital graphics, and plotters

- *Communication Devices* - Includes modem, encryption equipment, special interfaces, and error control

- *Storage Devices* - Includes magnetic tape (reel, cartridge, and cassette), floppy and hard disks, solid state (integrated circuits), and bubble and optical memories

Terminals - Three types of terminals are described below:

- *User Programmable* - Also called intelligent terminals, including the following:

  - Single-station or standalone
  - Multistation, shared processor
  - Teleprinter
  - Remote batch

- *User Nonprogrammable*

  - Single-station
  - Multistation, shared processor
  - Teleprinter

- *Limited Function* - Originally developed for specific needs, such as point-of-sale (POS), inventory data collection, controlled access, and other applications

Hardware Systems - Includes all processors from microcomputers to supercomputers. Hardware systems may require type- or model-unique operating software to be functional, but this category excludes applications software and peripheral devices, other than main memory and processors or CPUs not provided as part of an integrated (turnkey) system.

- *Microcomputer* - Combines all of the CPU, memory, and peripheral functions of an 8-, 16-, or 32-bit computer on a chip in various forms including:

  - Integrated circuit package

  - Plug-in boards with increased memory and peripheral circuits

  - Console including keyboard and interfacing connectors

  - Personal computer with at least one external storage device directly addressable by the CPU

  - An embedded computer which may take a number of shapes or configurations

- *Workstations* - High-performance, desktop, single-user computers employing (mostly) Reduced Instruction Set Computing (RISC). Workstations provide integrated, high-speed, local network-based services such as data base access, file storage and back-up, remote communications, and peripheral support. Typical workstation products are provided by Apollo (now a unit of Hewlett-Packard), Sun, Altos, DEC (the MicroVAX) and IBM. These products usually cost more than $15,000. However, at this writing many companies have recently announced sizable price cuts.

- *Midsize Systems* - Describe superminicomputers and the more traditional business minicomputers. Due to steadily improving design and technology, the latter have outgrown traditional definitions (which defined small systems as providing 32-bit to 64-bit word lengths at prices ranging from $15,000 to $350,000). Increasingly, minicomputers and workstations meet the 32-bit definition, and may go beneath the $15,000 lower price limit. Typical midrange systems include IBM System/3X, 43XX, AS/400, and 937X product lines, DEC PDP and VAX families (excluding MicroVAX families), and competitive products from a wide range of vendors, including HP, Data General, Wang, AT&T, Prime Concurrent, Gould, Unisys, NCR, Bull, Harris, Tandem, Stratus, and many others.

- *Large Computer* - Presently centered on storage controllers, but likely to become bus-oriented and to consist of multiple processors or parallel processor. Intended for structured mathematical and signal processing and typically used with general purpose, Von Neumann-type processors for system control. This term usually refers to traditional mainframes and supercomputers.

- *Supercomputer* - High-powered processors with numerical processing throughput that is significantly greater than the fastest general purpose computers, with capacities in the 100-500 million floating point operations per second (MFLOPS) range. Newer supercomputers, with burst modes over 500 MFLOPS, main storage size up to 10 million words, and on-line storage in the one-to-four gigabyte class, are labeled Class V to Class VII in agency long-range plans. Supercomputers fit in one of two categories:

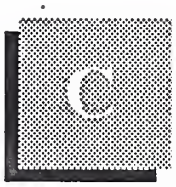
  - Real Time - Generally used for signal processing in military applications

  - Non-Real Time - For scientific use in one of three configurations:

    · Parallel processors
    · Pipeline processor
    · Vector processor

- *Supercomputer* - Is also applied to micro, mini, and large mainframe computers with performance substantially higher than attainable by Von Neumann architectures.

- *Embedded Computer* - Dedicated computer system designed and implemented as an integral part of a weapon, weapon system, or platform; critical to a military or intelligence mission such as command and control, cryptological activities, or intelligence activities. Characterized by military specifications (MIL SPEC) appearance and operation, limited but reprogrammable applications software, and permanent or semipermanent interfaces. These systems may vary in capacity from microcomputers to parallel processor computer systems.



Glossary of Federal Acronyms

The federal government's procurement language uses a combination of acronyms, phrases, and words that is complicated by different agency definitions and interpretations. The government also uses terms of accounting, business, economics, engineering, and law with new applications and technology.

Acronyms and contract terms that INPUT encountered most often in program documentation and interviews for this report are included here, but this glossary should not be considered all-inclusive. Federal procurement regulations (DAR, FPR, FAR, FIRMR, FPMR) and contract terms listed in RFIs, RFPs, and RFQs provide applicable terms and definitions.

Federal agency acronyms have been included to the extent they are employed in this report.

A

Federal Acronyms

AAS	Automatic Addressing System.
AATMS	Advanced Air Traffic Management System.
ACS	Advanced Communications Satellite (formerly NASA 30/20 GHz Satellite Program).
ACT-1	Advanced Computer Techniques (Air Force).
Ada	DoD High-Order Language.
ADA	Airborne Data Acquisition.
ADL	Authorized Data List.
ADNET	Anti-Drug Network.
ADS	Automatic Digital Switches (DCS).
AFA	Air Force Association.
AFCEA	Armed Forces Communications Electronics Association.
AGE	Aerospace Ground Equipment.
AIP	Array Information Processing.

AIS	Automated Information System.
AMD	Acquisition Management Directorate.
AMPE	Automated Message Processing Equipment.
AMPS	Automated Message Processing System.
AMSL	Acquisition Management Systems List.
ANG	Army National Guard
AP(P)	Advance Procurement Plan.
Appropriation	Congressionally approved funding for authorized programs and activities of the Executive Branch.
APR	Agency Procurement Request.
ARC	Acquisition Review Council.
ARPANET	DARPA network of scientific computers.
ASP	Aggregated Switch Procurement
ATLAS	Abbreviated Test Language for All Systems (for ATE-Automated Test Equipment).
Authorization	In the legislative process programs, staffing, and other routine activities must be approved by Oversight Committees before the Appropriations Committee will approve the money from the budget.
AUSA	Association of the U.S. Army.
AUTODIN	AUTOmatic DIgital Network of the Defense Communications System.
AUTOSEVOCOM	AUTOmatic SEcure VOice COMmunications Network
AUTOVON	AUTOmatic VOice Network of the Defense Communications System.
BA	Basic Agreement.
BAFO	Best And Final Offer.
Base level	Procurement, purchasing, and contracting at the military installation level.
BCA	Board of Contract Appeals.
Benchmark	Method of evaluating ability of a candidate computer system to meet user requirements.
Bid protest	Objection (in writing, before or after contract award) to some aspect of a solicitation by a valid bidder.
BML	Bidders Mailing List—qualified vendor information filed annually with federal agencies to automatically receive RFPs and RFQs in areas of claimed competence.
BOA	Basic Ordering Agreement.
B&P	Bid and Proposal—vendor activities in response to government solicitation/specific overhead allowance.
BPA	Blanked Purchase Agreement.
Budget	Federal Budget, proposed by the President and subject to Congressional review.
C^2	Command and Control.
C^3	Command, Control, and Communications.
C^4	Command, Control, Communications, and Computers.
C^3I	Command, Control, Communications, and Intelligence.
CAB	Contract Adjustment Board or Contract Appeals Board.
CADE	Computer-Aided Design and Engineering.
CADS	Computer-Assisted Display Systems.
CAIS	Computer-Assisted Instruction System.

CALS	Computer-Aided Logistics Support.
CAPS	Command Automation Procurement Systems.
CAS	Contract Administration Services or Cost Accounting Standards.
CASB	Cost Accounting Standards Board.
CASP	Computer-Assisted Search Planning.
CBD	*Commerce Business Daily*—U.S. Department of Commerce publication listing government contract opportunities and awards.
CBO	Congressional Budget Office.
CCEP	Commercial Comsec Endorsement Program
CCDR	Contractor Cost Data Reporting.
CCN	Contract Change Notice.
CCPDS	Command Center Processing and Display Systems.
CCPO	Central Civilian Personnel Office.
CDR	Critical Design Review.
CDRL	Contractor Data Requirement List.
CFE	Contractor-Furnished Equipment.
CFR	Code of Federal Regulations.
CICA	Competition in Contracting Act
CIG	Computerized Interactive Graphics.
CIM	Corporate Information Management or Center for Information Management.
CINCs	Commanders-in-Chief.
CIR	Cost Information Reports.
CM	Configuration Management.
CMI	Computer-Managed Instruction.
CNI	Communications, Navigation, and Identification.
CO	Contracting Office, Contract Offices, or Change Order.
COC	Certificate of Competency (administered by the Small Business Administration).
COCO	Contractor-Owned, Contractor-Operated.
CODSIA	Council of Defense and Space Industry Associations.
COMSTAT	Communications Satellite Corporation.
CONUS	CONtinental United States.
COP	Capability Objective Package.
COTR	Contracting Officer's Technical Representative.
COTS	Commercial Off-the-Shelf (Commodities).
CP	Communications Processor.
CPAF	Cost-Plus-Award-Fee Contract.
CPFF	Cost-Plus-Fixed-Fee Contract.
CPIF	Cost-Plus-Incentive-Fee Contract.
CPR	Cost Performance Reports.
CPSR	Contractor Procurement System Review.
CR	Cost Reimbursement (Cost Plus Contract).
CSA	Combat or Computer Systems Architecture.
CSIF	Communications Services Industrial Fund.
C/SCSC	Cost/Schedule Control System Criteria (also called "C-Spec").
CWAS	Contractor Weighted Average Share in Cost Risk.

DAB	Defense Acquisition Board.
DABBS	Defense Acquisition Bulletin Board System.
DAL	Data Accession List.
DAR	Defense Acquisition Regulations.
DARPA	Defense Advanced Research Projects Agency.
DAS	Data Acquisition System.
DBHS	Data Base Handling System.
DBOF	Defense Business Operating Fund.
DCA	Defense Communications Agency (see DISA).
DCAA	Defense Contract Audit Agency.
DCAS	Defense Contract Administration Services.
DCASR	DCAS Region.
DCC	Digital Control Computer.
DCP	Development Concept Paper (DoD).
DCS	Defense Communications System.
DCTN	Defense Commercial Telecommunications Network.
DDA	Dynamic Demand Assessment (Delta Modulation).
DDC	Defense Documentation Center.
DDI	Director of Defense Information.
DDL	Digital Data Link—A segment of a communications network used for data transmission in digital form.
DDN	Defense Data Network.
DDS	Defense Distribution System.
DECCO	DEfense Commercial Communications Office.
DECEO	DEfense Communications Engineering Office.
D&F	Determination and Findings—required documentation for approval of a negotiated procurement.
DFAS	Defense Finance and Accounting Service.
DIA	Defense Intelligence Agency.
DIF	Document Interchange Format, Navy-sponsored word processing standard.
DISA	Defense Information Systems Agency (Formerly DCA).
DHHS	Department of Health and Human Services.
DIDS	Defense Integrated Data Systems.
DISC	Defense Industrial Supply Center.
DLA	Defense Logistics Agency.
DMA	Defense Mapping Agency.
DMR	Defense Management Review.
DMRD	Defense Management Review Decision.
DNA	Defense Nuclear Agency.
DO	Delivery Order.
DOA	Department of Agriculture (also USDA).
DOC	Department of Commerce.
DOE	Department of Energy.
DOI	Department of Interior.
DOJ	Department of Justice.
DOS	Department of State.
DOT	Department of Transportation.
DPA	Delegation of Procurement Authority (granted by GSA under FPRs).

DPC	Defense Procurement Circular.
DQ	Definite Quantity Contract.
DQ/PL	Definite Quantity Price List Contract.
DR	Deficiency Report.
DRFP	Draft Request For Proposal.
DSCS	Defense Satellite Communication System.
DSN	Defense Switched Network.
DSP	Defense Support Program (WWMCCS).
DSS	Defense Supply Service.
DTC	Design-To-Cost.
DTN	Defense Transmission Network.
ECP	Engineering Change Proposal.
ED	Department of Education.
EEO	Equal Employment Opportunity.
8(a) Set-Aside	Agency awards direct to Small Business Administration for direct placement with a socially/economically disadvantaged company.
EMC	Electro-Magnetic Compatibility.
EMCS	Energy Monitoring and Control System.
EO	Executive Order—Order issued by the President.
EOQ	Economic Ordering Quantity.
EPA	Economic Price Adjustment.
EPA	Environmental Protection Agency.
EPMR	Estimated Peak Monthly Requirement.
EPS	Emergency Procurement Service (GSA) or Emergency Power System.
EUC	End User Computing, especially in DoD.
FA	Formal Advertising.
FAC	Facility Contract.
FAR	Federal Acquisition Regulations.
FCA	Functional Configuration Audit.
FCC	Federal Communications Commission.
FCDC	Federal Contract Data Center.
FCRC	Federal Contract Research Center.
FDPC	Federal Data Processing Center.
FEDSIM	Federal (Computer) Simulation Center (GSA).
FEMA	Federal Emergency Management Agency.
FFP	Firm Fixed-Price Contract (also Lump Sum Contract).
FIPR	Federal Information Processing Resource.
FIPS	NBS Federal Information Processing Standard.
FIPS PUBS	FIPS Publications.
FIRMR	Federal Information Resource Management Regulations.
FMS	Foreign Military Sales.
FOC	Final Operating Capability.
FOIA	Freedom of Information Act.
FP	Fixed-Price Contract.
FP-L/H	Fixed-Price—Labor/Hour Contract.
FP-LOE	Fixed-Price—Level-Of-Effort Contract.

FPMR	Federal Property Management Regulations.
FPR	Federal Procurement Regulations.
FSC	Federal Supply Classification.
FSG	Federal Supply Group.
FSN	Federal Supply Number.
FSS	Federal Supply Schedule or Federal Supply Service (GSA).
FSTS	Federal Secure Telecommunications System.
FT Fund	A revolving fund, designated as the Federal Telecommunications Fund, used by GSA to pay for GSA-provided common-user services, specifically including the current FTS and proposed FTS 2000 services.
FTSP	Federal Telecommunications Standards Program administered by NCS; Standards are published by GSA.
FTS	Federal Telecommunications System.
FTS 2000	Replacement of the Federal Telecommunications System.
FY	Fiscal Year.
FYDP	Five-Year Defense Plan.
GAO	General Accounting Office.
GFE	Government-Furnished Equipment.
GFM	Government-Furnished Material.
GFY	Government Fiscal Year (October to September).
GIDEP	Government-Industry Data Exchange Program.
GOCO	Government Owned—Contractor Operated.
GOGO	Government Owned—Government Operated.
GOSIP	Government Open Systems Interconnection Profile.
GPO	Government Printing Office.
GPS	Global Positioning System.
GRH	Gramm-Rudman-Hollings Act (1985), also called Gramm-Rudman Deficit Control.
GS	General Schedule.
GSA	General Services Administration.
GSBCA	General Services Administration Board of Contract Appeals.
HCFA	Health Care Financing Administration.
HHS	(Department of) Health and Human Services.
HPA	Head of Procuring Activity.
HSDP	High-Speed Data Processors.
HUD	(Department of) Housing and Urban Development.
I-CASE	Integrated Computer-Aided Software Engineering.
IAR	Senior IRM Official.
ICA	Independent Cost Analysis.
ICAM	Integrated Computer-Aided Manufacturing.
ICE	Independent Cost Estimate.
ICP	Inventory Control Point.
ICST	Institute for Computer Sciences and Technology, National Bureau of Standards, Department of Commerce.
IDAMS	Image Display And Manipulation System.

IDEP	Interservice Data Exchange Program.
IDIQ	Indefinite Delivery-Indefinite Quantity.
IDN	Integrated Data Network.
IFB	Invitation For Bids.
IOC	Initial Operating Capability.
IOI	Internal Operating Instructions.
IPS	Integrated Procurement System.
IQ	Indefinite Quantity Contract.
IR&D	Independent Research & Development.
IRM	Information Resources Management.
IXS	Information Exchange System.
JCS	Joint Chiefs of Staff.
JCALS	Joint Computer-Aided Logistics Support.
JFMIP	Joint Financial Management Improvement Program.
JOCIT	Jovial Compiler Implementation Tool.
JSIPS	Joint Systems Integration Planning Staff.
JSOP	Joint Strategic Objectives Plan.
JSOR	Joint Service Operational Requirement.
JUMPS	Joint Uniform Military Pay System.
JWAM	Joint WWMCCS ADP Modernization (Program).
LC	Letter Contract.
LCC	Life Cycle Costing.
LCMP	Life Cycle Management Procedures (DD7920.1).
LCMS	Life Cycle Management System.
L-H	Labor-Hour Contract.
LOI	Letter of Interest.
LRPE	Long-Range Procurement Estimate.
LRIRP	Long-Range Information Resource Plan.
LTD	Live Test Demonstration.
MAISRC	Major Automated Information Systems Review Council (DoD).
MANTECH	MANufacturing TECHnology.
MAPS	Multiple Address Processing System.
MAP/TOP	Manufacturing Automation Protocol/Technical and Office Protocol.
MASC	Multiple Award Schedule Contract.
MDA	Multiplexed Data Accumulator.
MENS	Mission Element Need Statement or Mission Essential Need Statement (see DD-5000.1 Major Systems Acquisition).
MILSCAP	Military Standard Contract Administration Procedures.
MIL SPEC	Military Specification.
MIL STD	Military Standard.
MIPR	Military Interdepartmental Purchase Request.
MLS	Multilevel Security.
MNF	Multi-National Force.
MOD	Modification.
MOL	Maximum Ordering Limit (Federal Supply Service).

MPC	Military Procurement Code.
MYP	Multi-Year Procurement.
NARDIC	Navy Research and Development Information Center.
NASA	National Aeronautics and Space Administration.
NBS	National Bureau of Standards.
NCA	National Command Authorities.
NCMA	National Contract Management Association.
NCS	National Communications System (evolving to DISN).
NICRAD	Navy-Industry Cooperative Research and Development.
NIP	Notice of Intent to Purchase.
NIST	National Institute for Standards and Technology (Nee: NBS)
NMCS	National Military Command System.
NSA	National Security Agency.
NSEP	National Security and Emergency Preparedness.
NSF	National Science Foundation.
NSIA	National Security Industrial Association.
NTIA	National Telecommunications and Information Administration of the Department of Commerce; (replaced the Office of Telecommunications Policy in 1970).
NTIS	National Technical Information Service.
Obligation	"Earmarking" of specific funding for a contract from committed agency funds.
OCS	Office of Contract Settlement.
OFCC	Office of Federal Contract Compliance.
Off-Site	Services to be provided near but not in government facilities.
OFMP	Office of Federal Management Policy (GSA).
OFPP	Office of Federal Procurement Policy.
OIRM	Office of Information Resources Management.
O&M	Operations & Maintenance.
OMB	Office of Management and Budget.
O,M&R	Operations, Maintenance, and Readiness.
On-Site	Services to be performed on a government installation or in a specified building.
OPM	Office of Procurement Management (GSA) or Office of Personnel Management.
Options	Sole-source additions to the base contract for services or goods to be exercised at the government's discretion.
OSADBU	Office of Small and Disadvantaged Businesses.
OSHA	Occupational Safety and Health Act.
OSI	Open System Interconnect.
OSP	Offshore Procurement.
OTA	Office of Technology Assessment (Congress).
Out-Year	Proposed funding for fiscal years beyond the Budget Year (next fiscal year).
P-1	FY Defense Production Budget.
P3I	Pre-Planned Product Improvement (program in DoD).
PAR	Procurement Authorization Request or Procurement Action Report.
PAS	Pre-Award Survey.
PASS	Procurement Automated Source System.
PCO	Procurement Contracting Officer.
PDA	Principal Development Agency.

PDM	Program Decision Memorandum.
PDR	Preliminary Design Review.
PIR	Procurement Information Reporting.
PME	Performance Monitoring Equipment.
PMP	Purchase Management Plan.
PO	Purchase Order or Program Office.
POE	Panel Of Experts.
POM	Program Objective Memorandum.
POSIX	Portable Open System Interconnection Exchange.
POTS	Purchase of Telephone Systems.
PPBS	Planning, Programming, Budgeting System.
PR	Purchase Request or Procurement Requisition.
PRA	Paperwork Reduction Act.
PS	Performance Specification—alternative to a Statement of Work, when work to be performed can be clearly specified.
QA	Quality Assurance.
QAO	Quality Assurance Office.
QMCS	Quality Monitoring and Control System (DoD software).
QMR	Qualitative Material Requirement (Army).
QPL	Qualified Products List.
QRC	Quick Reaction Capability.
QRI	Quick Reaction Inquiry.
R-1	FY Defense RDT&E Budget.
RAM	Reliability, Availability, and Maintainability.
RC	Requirements Contract.
R&D	Research and Development.
RDA	Research, Development, and Acquisition.
RDD	Required Delivery Date.
RD&E	Research, Development, and Engineering.
RDF	Rapid Deployment Force.
RDT&E	Research, Development, Test, and Engineering.
RFI	Request For Information.
RFP	Request For Proposal.
RFQ	Request For Quotation.
RFTP	Request For Technical Proposals (Two-Step).
ROC	Required Operational Capability.
ROI	Return On Investment.
RTAS	Real Time Analysis System.
RTDS	Real Time Display System.
SA	Supplemental Agreement.
SADBU	Small and Disadvantaged Business Utilization.
SBA	Small Business Administration.
SB Set-Aside	Small Business Set-Aside contract opportunities with bidders limited to certified small businesses.
SCA	Service Contract Act (1964 as amended).

SCN	Specification Change Notice.
SDN	Secure Data Network.
SEC	Securities and Exchange Commission.
SE&I	Systems Engineering and Integration.
SETA	Systems Engineering/Technical Assistance.
SETS	Systems Engineering/Technical Support.
SIBAC	Simplified Intragovernmental Billing and Collection System.
SIMP	Systems Integration Master Plan.
SIOP	Single Integrated Operations Plan.
Sole Source	Contract award without competition.
Solicitation	Invitation to submit a bid.
SOR	Specific Operational Requirement.
SOW	Statement of Work.
SSA	Source Selection Authority (DoD).
SSAC	Source Selection Advisory Council.
SSEB	Source Selection Evaluation Board.
SSO	Source Selection Official (NASA).
STINFO	Scientific and Technical INFOrmation Program—Air Force/NASA.
STU	Secure Telephone Unit.
SWO	Stop-Work Order.
Synopsis	Brief Description of contract opportunity in CBD after D&F and before release of solicitation.
TA/AS	Technical Assistance/Analysis Services.
TCP/IP	Transmission Control Protocol/Internet Protocol.
TEMPEST	Studies, inspections, and tests of unintentional electromagnetic radiation from computer, communication, command, and control equipment that may cause unauthorized disclosure of information; usually applied to DoD and security agency testing programs.
TILO	Technical and Industrial Liason Office—Qualified Requirement Information Program—Army.
TM	Time and Materials contract.
TOA	Total Obligational Authority (Defense).
TOD	Technical Objective Document.
TQM	Total Quality Management.
TR	Temporary Regulation (added to FPR, FAR).
TRACE	Total Risk Assessing Cost Estimate.
TRCO	Technical Representative of the Contracting Offices.
TREAS	Department of Treasury.
TRP	Technical Resources Plan.
TSP	GSA's Teleprocessing Services Program.
TVA	Tennessee Valley Authority.
UCAS	Uniform Cost Accounting System.
USA	U.S. Army.
USAF	U.S. Air Force.
USCG	U.S. Coast Guard.
USMC	U.S. Marine Corps.

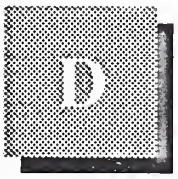
USN	U.S. Navy.
U.S.C.	United States Code.
USPS	United States Postal Service.
USRRB	United States Railroad Retirement Board.
VA	Veterans Affairs Department.
VE	Value Engineering.
VHSIC	Very High Speed Integrated Circuits.
VIABLE	Vertical Installation Automation BaseLine (Army).
VICI	Voice Input Code Identifier.
VTC	Video Teleconferencing.
WAM	WWMCCS ADP Modernization Program.
WBS	Work Breakdown Structure.
WGM	Weighted Guidelines Method.
WIN	WWMCCS Intercomputer Network.
WITS	Washington Interagency Telecommunications System.
WIS	WWMCCS Information Systems.
WS	Work Statement—Offerer's description of the work to be done (proposal or contract).
WWMCCS	World-Wide Military Command and Control System.

B

General and Industry Acronyms

ADAPSO	Association of Data Processing Service Organization, now the Computer Software and Services Industry Association. (See ITAA).
ADP	Automatic Data Processing.
ADPE	Automatic Data Processing Equipment.
ANSI	American National Standards Institute.
BOC	Bell Operating Company.
CAD	Computer-Aided Design.
CAM	Computer-Aided Manufacturing.
CASE	Computer-Aided Software Engineering.
CBEMA	Computer and Business Equipment Manufacturers Association.
CCIA	Computers and Communications Industry Association.
CCITT	Comite Consultatif Internationale de Télégraphique et Téléphonique; Committee of the International Telecommunication Union.
COBOL	COmmon Business-Oriented Language.
COS	Corporation for Open Systems.
CPU	Central Processor Unit.
DMBS	Data Base Management System.
DRAM	Dynamic Random Access Memory.

EIA	Electronic Industries Association.
EPROM	Erasible Programmable Read-Only Memory.
IEEE	Institute of Electrical and Electronics Engineers.
ISDN	Integrated Services Digital Networks.
ISO	International Organization for Standardization; voluntary international standards organization and member of CCITT.
ITAA	Information Technology Association of America (Formerly ADAPSO).
ITU	International Telecommunication Union.
LSI	Large-Scale Integration.
MFJ	Modified Final Judgement.
PROM	Programmable Read-Only Memory.
RBOC	Regional Bell Operating Company.
UNIX	AT&T Proprietary Operating System.
UPS	Uninterruptable Power Source.
VAR	Value-Added Reseller.
VLSI	Very Large-Scale Integration.
WORM	Write-Once-Read-Many-Times.



Policies, Regulations, and Standards

A

OMB Circulars

A-11	Preparation and Submission of Budget Estimates.
A-49	Use of Management and Operating Contracts.
A-71	Responsibilities for the Administration and Management of Automatic Data Processing Activities.
A-109	Major Systems Acquisitions.
A-120	Guidelines for the Use of Consulting Services.
A-121	Cost Accounting, Cost Recovery, and Integrated Sharing of Data Processing Facilities.
A-123	Internal Control Systems.
A-127	Financial Management Systems.
A-130	Management of Federal Information Resources.
A-131	Value Engineering.

B

GSA Publications

The FIRMR as published by GSA is the primary regulation for use by federal agencies in the management, acquisition, and use of both ADP and telecommunications information resources.

C

DoD Directives

DD-5000.1	Major System Acquisitions.
DD-5000.2	Major System Acquisition Process.
DD-5000.11	DoD Data Administration (C3I).
DD-5000.31	Interim List of DoD-Approved, High-Order Languages.
DD-5000.35	Defense Acquisition Regulatory Systems.
DD-5200.1	DoD Information Security Program.

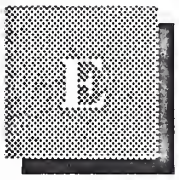
DD-5200.28	Security Requirements for Automatic Data Processing (ADP) Systems.
DD-5200.28-M	Manual of Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource Sharing ADP Systems.
DD-7920.2	Major Automated Information Systems Approval Process.
DD-7935	Automated Data Systems (ADS) Documentation.
DoDD 3405.1	Computer Programming Language Policy
DoDD 5000.11	DoD Data administration (C31)
DoDI 5000.12	Data Elements and Data Codes Standardization Procedure
DoDI 5000.18	Implementation of Standard Data Elements and Related Features
DoDD 5105.19	Defense Information Systems Agency
DoDD 5110.4	Washington Headquarters Services
DoDD 5118.3	Comptroller of the Department of Defense
DoDD 5137.1	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
DoDD 7740.1	DoD Information Resources Management Program
DoD 7740.1-G	DoD ADP Internal Control Guideline
DoDD 7740.2	Automated Information System (AIS) Strategic Planning
DoDI 7740.3	Information Resources Management (IRM) Review Program
DoDD 7750.5	Management and Control of Information Requirements
DoDI 7750.7	DoD Forms Management Program
DoDI 7920.2-M	Automated Information Systems (AIS) Life-Cycle Manual
DoDI 7920.4	Baselining of Automated Information Systems (AISs)
DoDI 7920.5	Management of End User Computing (EUC)
DoDI 7930.1	Information Technology Users Group Program
DoDI 7930.2	ADP Software Exchange and Release
DoDD 7950.1	Automated Data Processing Resources Management
DoD 7950.1-M	Defense Automated Resources Management Manual of Information Requirements

D
Standards

ADCCP	Advanced Data Communications Control Procedures; ANSI Standard X3.66 of 1979; also NIST FIPS 71.
CCITT G.711	International PCM standard.
CCITT T.0	International standard for classification of facsimile apparatus for document transmission over telephone-type circuits.

DEA-1	Proposed ISO standard for data encryption based on the NIST DES.
EIA RS-170	Monochrome video standard.
EIA RS-170A	Color video standard.
EIA RS-464	EIA PBX standards.
EIA RS-465	Standard for Group III facsimile.
EIA RS-466	Facsimile standard; procedures for document transmission in the General Switched Telephone Network.
EIA RS-232-C	EIA DCE to DTE interface standard using a 25-Pin connector; similar to CCITT V-24.
EIA RS-449	New EIA standard DTE to DCE interface which re places RS-232-C.
FED-STD 1000	Proposed Federal Standard for adoption of the full OSI reference model.
FED-STD 1026	Federal Data Encryption Standard (DES) adopted in 1983; also FIPS 46.
FED-STD 1041	Equivalent to FIPS 100.
FED-STD 1061	Group II Facsimile Standard (1981).
FED-STD 1062	Federal standard for Group III facsimile; equivalent to EIA RS-465.
FED-STD 1063	Federal facsimile standard; equivalent to EIA RS-466.
FED-STDs 1005, 1005A-1008	Federal Standards for DCE Coding and Modulation.
FIPS 46	NIST Data Encryption Standard (DES).
FIPS 81	DES Modes of Operation.
FIPS 100	NIST Standard for packet-switched networks; subset of 1980 CCITT X.25.
FIPS 107	NIST Standard for local-area networks, similar to IEEE 802.2 and 802.3.
FIPS 146	Government Open Systems Interconnection (OSI) Profile (GOSIP).
FIPS 151	NIST POSIX (Portable Operating System Interface for UNIX) standard.
IEEE 802.2	OSI-Compatible IEEE standard for data-link control in local-area networks.
IEEE 802.3	Local-area network standard similar to Ethernet.
IEEE 802.4	OSI-compatible standard for token bus local-area networks.
IEEE 802.5	Local-area networks standard for token ring networks.
IEEE P1003.1	POSIX standard, similar to FIPS 151.

MIL-STD-188-114C	Physical interface protocol similar to RS-232 and RS-449.
MIL-STD-1777	IP-Internet Protocol.
MIL-STD-1778	TCP - Transmission Control Protocol.
MIL-STD-1780	File Transfer Protocol.
MIL-STD-1781	Simple Mail Transfer Protocol (electronic mail).
MIL-STD-1782	TELNET - virtual terminal protocol.
MIL-STD-1815A	Ada Programming Language Standard.
SVID	UNIX System Interface Definition.
X.12	ANSI standard for Electronic Data Interchange
X.21	CCITT standard for interface between DTE and DCE for synchronous operation on public data networks.
X.25	CCITT standard for interface between DTE and DCE for terminals operating in the packet mode on public data networks.
X.75	CCITT standard for links that interface different packet networks.
X.400	ISO application-level standard for the electronic transfer of messages (electronic mail).



Related INPUT Reports

A
Annual Market Analyses

U.S. Information Services Vertical Markets, 1991

U.S. Information Services Cross-Industry Markets, 1991

Procurement Analysis Reports, GFY 1992-1997

U.S. Network Services Market, 1991-1996

B
Market Reports

Federal Network Management, 1991-1996

Federal Computer Equipment Market, 1991-1996

Federal Electronic Imaging Market, 1991-1996

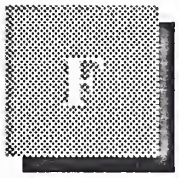
U.S. Electronic Commerce/EDI Federal Markets, 1991-1996

Federal Systems Integration Market, 1991-1996

Federal Professional Services Markets, 1991-1996

Federal Telecommunications Market, 1992-1997

Federal Computer Security Market, 1990- 1995



INPUT Questionnaire— Federal Agencies

This questionnaire is directed to the study of the federal market for hardware, software and services to support federal security concerns. It also focuses on the present and future compliance with the Computer Security Act of 1987 and other regulations.

Interviewer: _____

Respondent Name: _____

Title: _____ Phone: _____

Department: _____ Agency: _____

Address: _____

Office Code: _____

Function: _____

Referrals: _____

Confidential

Agency Questionnaire—Federal Computer Security Market

1a. With respect to the Computer Security Act of 1987, what computer security measures have already been adapted by your agency?

- ❑ Identified all systems with sensitive information
- ❑ Completed security plans for each system
- ❑ Security implementation

1b. What measures are planned for the next 2-5 years?

_____

_____

_____

2. In your opinion, what type of computers are most vulnerable to security problems?
Microcomputers ❑ Mainframes ❑ Midsize ❑
Why?

_____

_____

_____

3. Since the publicity concerning "computer viruses," what steps if any, has your agency taken to protect your computers?

_____

_____

_____

4. What additional directives and guidelines regarding computer security does your agency use in addition to the Computer Security Act?

_____

_____

_____

5a. What responsibilities does your staff have for implementing computer security?

5b. What computer security training requirements has your organization initiated for its employees?

6a. How has the increase in end-user computing impacted your agency's computer security plans and operations?

6b. How has greater employee awareness of computer security contributed to additional agency requirements for training support?

7a. What do you perceive are the major threats to your system(s)?

- ❑ Site access and damage
- ❑ Data access (disclosure of private, classified, or proprietary data)
- ❑ Data manipulation (file alteration)
- ❑ Software or system manipulation (computer viruses)
- ❑ Other (_____)

7b. What are the functional requirements of your agency's/organization's computer security system?

- ❑ Network security
- ❑ End-user computer or computing access
- ❑ Physical security
  - ❑ Computer center
  - ❑ Remote processing site
  - ❑ PCs in LAN or WAN site
- ❑ Data security
- ❑ Other (_____)

8a. What performance criteria has your agency established for computer security products?

_____

_____

_____

8b. How successful have industry products and services been in meeting the current criteria?

_____

_____

_____

9. What might be the impact of the computer security regulations and policies on the following?
a. Open System Architecture

_____

_____

b. GOSIP

_____

_____

c. CALS Initiatives

_____

_____

d. EDI Initiatives

_____

_____

10a. Which of the following computer security products and services does your agency/organization plan to acquire through FY 1993? *(Check all that apply)*

- ❑ Data encryption equipment
- ❑ Software-driven password security
- ❑ Secure networking products
- ❑ Emission control devices
- ❑ Secure workstations
- ❑ Security training tools
- ❑ Tempest products
- ❑ Risk management analysis
- ❑ Communications security products
- ❑ Secure UNIX-based products
- ❑ Contractor assistance for preparation of plans
- ❑ Other contractor support
- ❑ Other computer security devices

10b. Have you or do you intend to use a GSA contractor to support your security needs?

Yes ❑ No ❑

If yes, which contractor and in what way?

_____

_____

_____

11. On a scale of 1-5, with 5 being very important and 1 being not important, please rate the following selection criteria for computer security products and services.

Criteria	Rating				
Encryption features	1	2	3	4	5
Vendor's federal experience	1	2	3	4	5
Password systems	1	2	3	4	5
Ease of implementation	1	2	3	4	5
Vendor's support reputation	1	2	3	4	5
Product price	1	2	3	4	5
Secure network capabilities	1	2	3	4	5
Training features	1	2	3	4	5
Other_____	1	2	3	4	5

12a. In your opinion, who are the most important vendors in the federal computer security market? *(Specify vendor names)*

_____

_____

_____

12b. How do you see the market developing? (i.e., civilian vs. defense-oriented companies, etc.)

_____

_____

_____

13. Which methods of acquisition does your agency use for its purchase of computer security products ? *(Please check all that apply and circle method used most often.)*

- ❑ GSA Schedules
- ❑ RFP for requirement contract
- ❑ RFPs for specific purchase
- ❑ Purchase security devices as part of other procurements
- ❑ Other (_____)

14. What type of vendor or organization appears most appropriate for providing computer security products/services for your agency (organization)?

Hardware vendors	❑	Professional services firms	❑
Software vendors	❑	Systems integrators	❑
Aerospace divisions	❑	Not-for-profit firms	❑
Other (_____)	❑		

15. Any suggestions for improvements to security products or services offered by vendors?

_____

_____

_____

16. How would you rate the following computer security vendor characteristics with respect to performance for your agency?
(1=Definitely not satisfactory, 2=Somewhat satisfactory, 3=Satisfactory, 4=Very satisfactory, 5=Outstanding performance)

Characteristic	Rating				
1. Encryption experience	1	2	3	4	5
2. Training experience	1	2	3	4	5
3. Successful implementation	1	2	3	4	5
4. Price	1	2	3	4	5
5. Staff experience	1	2	3	4	5
6. Hardware offered	1	2	3	4	5
7. Software offered	1	2	3	4	5
8. Support experience	1	2	3	4	5
9. Delivery schedule	1	2	3	4	5
10. Other (_____)	1	2	3	4	5

Impacts/Trends

17. How are technological changes affecting your agency's computer security requirements through FY 1993?

Technology	Impact
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

18. Could you please identify those industry or market factors (non-technical) that would have the greatest impact on your agency's computer security plans? Include industry mergers, business trends, etc.

_____

_____

_____

19. What impact, if any, have federal government budgetary constraints had on implementing the agency's computer security plans ?

20. How will government policies or regulations from each of the following government agencies impact your agency's/organization's computer security requirements and acquisitions through FY 1993?

a. NIST

b. NSA

c. GSA

Any other policy initiatives by regulatory or legislative organizations?

Report Quality Evaluation

To our clients:
To ensure that the highest standards of report quality are maintained, INPUT would appreciate your assessment of this report. Please take a moment to provide your evaluation of the usefulness and quality of this study. When complete, simply fold, staple, and drop in the mail. Postage has been pre-paid by INPUT if mailed in the U.S.

Thank You.

1. Report title: ***Federal Computer Security Market, 1992-1997*** (FISE2)

2. Please indicate your reason for reading this report:
   - ☐ Required reading
   - ☐ Area of high interest
   - ☐ Area of general interest
   - ☐ New product development
   - ☐ Business/market planning
   - ☐ Product planning
   - ☐ Future purchase decision
   - ☐ Systems planning
   - ☐ Other _____

3. Please indicate extent report used and overall usefulness:

	Extent		Usefulness (1=Low, 5=High)				
	Read	Skimmed	1	2	3	4	5
Executive Overview	☐	☐	☐	☐	☐	☐	☐
Complete report	☐	☐	☐	☐	☐	☐	☐
Part of report (_____ %)	☐	☐	☐	☐	☐	☐	☐

4. How useful were:

Data presented	☐	☐	☐	☐	☐
Analyses	☐	☐	☐	☐	☐
Recommendations	☐	☐	☐	☐	☐

5. How useful was the report in these areas:

Alert you to new opportunities or approaches	☐	☐	☐	☐	☐
Cover new areas not covered elsewhere	☐	☐	☐	☐	☐
Confirm existing ideas	☐	☐	☐	☐	☐
Meet expectations	☐	☐	☐	☐	☐
Other _____	☐	☐	☐	☐	☐

6. Which topics in the report were the most useful? Why? _____

_____

7. In what ways could the report have been improved? _____

_____

8. Other comments or suggestions: _____

_____

Name _____ Title _____

Department _____

Company _____

Address _____

City _____ State _____ ZIP _____

Telephone _____ Date completed _____

Thank you for your time and cooperation.

M&S 633/01 12/89

INPUT

STAPLE

FOLD HERE

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL
First Class Mail Permit No. 9070 Vienna, VA

POSTAGE WILL BE PAID BY ADDRESSEE

Attention: Marketing Department

INPUT
1953 Gallows Road, Suite 560
Vienna, VA 22182-9793

FOLD HERE